République du Tchad
Université Roi Fayçal
Faculté de Génie
Informatique et Technologie
de l'Information



جمهورية تشاد
جامعة الملك فيصل
كلية هندسة الحـاسوب
وتكنولوجيا المعلومات

بحث مقدم لاستكمال درجة الليسانس(المتريز) بعنوان:

أمـن طبقـة التــطبيـقـات

Security of Application Layer

إعداد الطالب:خيار محمود زكريا

إشراف:الدكتور/حسن عبد الله أبكر

العام الجامعي 2011-2012


بسم الله الرحمن الرحيم

(وَعَلَّمَكَ مَا لَمۡ تَكُن تَعۡلَمُۚ وَكَانَ فَضۡلُ ٱللَّهِ عَلَيۡكَ عَظِيمٗا)

سورة النساء:113

الإهداء

إلى من كل البشرية له تدين

إلى سيد الخلق محمد النبي

إلى من افديهم عمري و كل السنين

إلى الغاليين أمي و أبي

إلى من كانوا يضيئون لي الطريق

ويساندوني ويتنازلون عن حقوقهم

لإرضائي والعيش في هناء

إخوتي الأعزاء رفقاء الحياة

الشكر والتقدير

إن الشكر والحمد لله عز وجل الذي بلطفه ومنه الكريم تيسرت الأمور فأوجد الأسباب وقدر الأقدار.

انه من دواعي سروري وعميق عرفاني أن أقدم شكري وامتناني لأستاذي حسن عبد الله أبكر، لكل الجهود الكريمة التي بذلها بالإشراف على البحث طوال فتره التحضير.

وكل اعتزازي وشكري لأسرتي الغالية الذين هم أناروا لي دربي بالنصيحة والتشجيع والدعاء .

واشكر عميد كلية الحاسوب م.محمد بخاري، ومسجلها م. عمر عبد الرحمن، وجميع أفراد جامعة الملك فيصل من إداريين وهيئة تدريس وزملاء.

كما اشكر صديقي م.محمد نعيم الذي ساهم في انجاز البحث و أتمنى له التوفيق والنجاح في حياته.

واشكر كل من ساعدني وقدم لي النصيحة اسأل الله أن يجزيهم عني خير الجزاء.

مقدمة

بسم الله الرحمن الرحيم

إن الحمد لله نحمده و نستعينه، ونصلي ونسلم على نبينا محمد وآله وصحبه .

أما بعد...

فإن التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة في أساليب العمل،إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية و الدولية و أجهزة الحاسوب من الأمور الروتينية في عصرنا الحالي و إحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال و تطوير أساليب تخزين و نقل المعلومات حيث أن انتشار أنظمة المعلومات أدى إلى أن تكون عرضة للاختراق، لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على اقتناءه و توفير سبل الحماية له.

إن موضوع الأمن في طبقة التطبيقات يرتبط ارتباطا وثيقا بأمن الشبكات فلا يوجد أمن للتطبيقات إذا لم يراعى أمن الشبكات، و في ظل التطورات التي تحدث في العالم و التي أثرت على الإمكانيات التقنية المتقدمة المتاحة و الرامية إلى اختراق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية و الوقائية و حسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب، و كان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها.

إن هذا البحث يقدم حلا واقعياً للراغبين في فهم طرق تحقيق الأمن في طبقة التطبيقات و فهم أمن الشبكات على حد سواء، و قد اعتمدنا التدرج و عرض المعلومات بالتفصيل التقني عند الحاجة لكي يكون مرجع للطلاب و ليساهم مع غيره من الكتب السابقة في إضافة المزيد من البحوث للمكتبة العربية.

وما توفيقي إلا بالله عليه توكلت...

مختصر البحث:

يتناول هذا البحث أمن طبقة التطبيقات في النموذج المرجعيOSI، حيث نذكر مفاهيم عامة حول الشبكات وأنواعها ثم نوضح ما هو النموذج المرجعي ونتكلم عن طبقاته السبع ونعرف بطبقة التطبيقات،نتحدث عن مفهوم الأمن وبشكل خاص أمن الشبكات،والمخاطر التي تتعرض لها من فيروسات وهاكر وغيره، ثم نذكر طرق حماية البيانات من تشفير وتوقيع الكتروني، وشهادات رقمية ثم نتحول إلى موضوع بحثنا "أمن طبقة التطبيقات Security of Application Layers"

والتقنيات المستخدمة في أمنها:SSL،SMB،TLS،IPSCE،IDS،HASH.

ثم نتحدث عن الجدار الناري(Firewall) ودوره في حماية طبقة التطبيقات ثم المنطقة المحايدة(DMZ) ودورها مع الجدار الناري في توفير الحماية لطبقة التطبيقات.

أهداف البحث

يهدف هذا البحث إلى:

1. التطرق والوقوف على المخاطر التي تتعرض لها الشبكة وخاصة في طبقة التطبيقات Application Layer.
2. كيفية حماية التطبيقات من المخاطر المختلفة .
3. معرفة الوسائل والتقنيات المستخدمة في تامين التطبيقات.

أهمية البحث

تكمن أهمية البحث في النقاط التالية:

1. يتطرق لأمن طبقة التطبيقات باعتبارها الطبقة التي تشكل الواجهة الأساسية التي تتعامل معها برامج المستخدم كمتصفح الويب وغيرها.
2. تعتمد تطبيقات المستخدم النهائية على البروتوكولات في طبقة التطبيقات لأداء وظيفة شبكية معينة.
3. يوضح أنه في حالة تعرض طبقة التطبيقات لاختراق أو تعديل غير مرخص له فانه يتم التغيير و التأثير في موارد الشبكة.

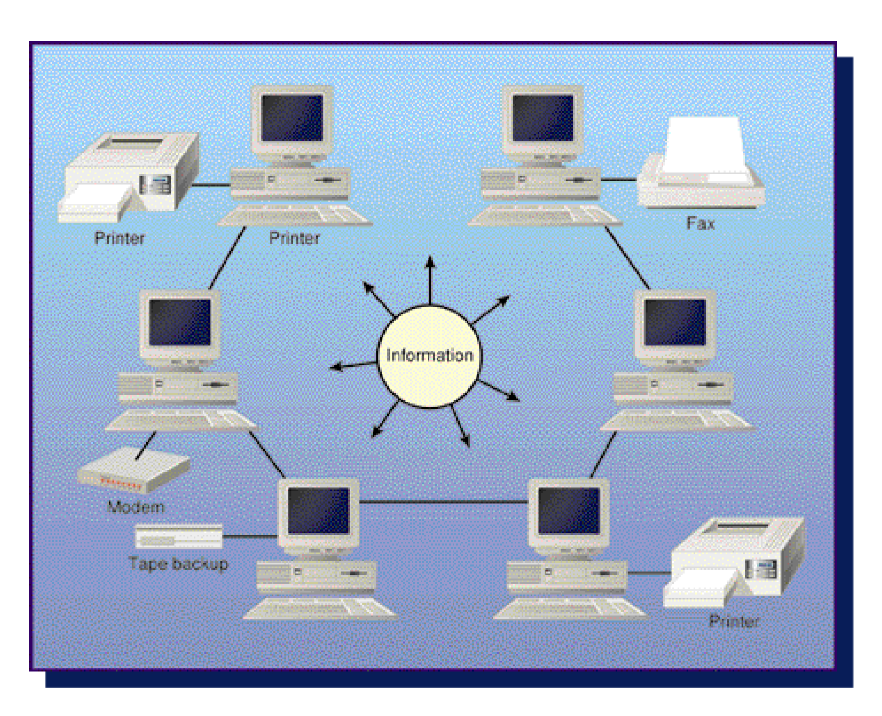
الفصـــــــــــل الأول

تعريف الشبكات والنموذج المرجعي

الفصل الأول: مفاهيم حول الشبكات

1.1 تعريف شبكة الحاسبات

الشبكة هي عبارة عن مجموعة حاسبات متنوعة و مختلفة (طرفيات، حاسبات شخصية، محطات عمل، حاسبات متوسطة، حاسبات كبيرة أو عملاقة) مرتبطة ببعضها البعض و ذلك عن طريق وحدات ربط (Network Cards) ووسائط (من كوابل محوريةCoaxial Cable، أسلاك مجدولة Twisted Pair وألياف ضوئية Optic Fiber) و أجهزة ملحقة (مثل جهاز تقويةamplifier أو، مكررRepeater، مجمعات توصيلHub ، جسر أو مسار ربطBridge) مكونة بذلك شبكة، متكاملة[4]. و بهذه الطريقة يمكن لأي حاسب أن يستفيد من الخدمات التي تقدمها الحاسبات الأخرى المرتبطة مع الشبكة حيث انه يندر حاليا استخدام الحاسب بمعزل عن الحاسبات الأخرى. أنظر الشكل (1.1.)



الشكل (1.1): يمثل الشبكات واستخدامها[4]

2.1. أهداف شبكات الحاسبات

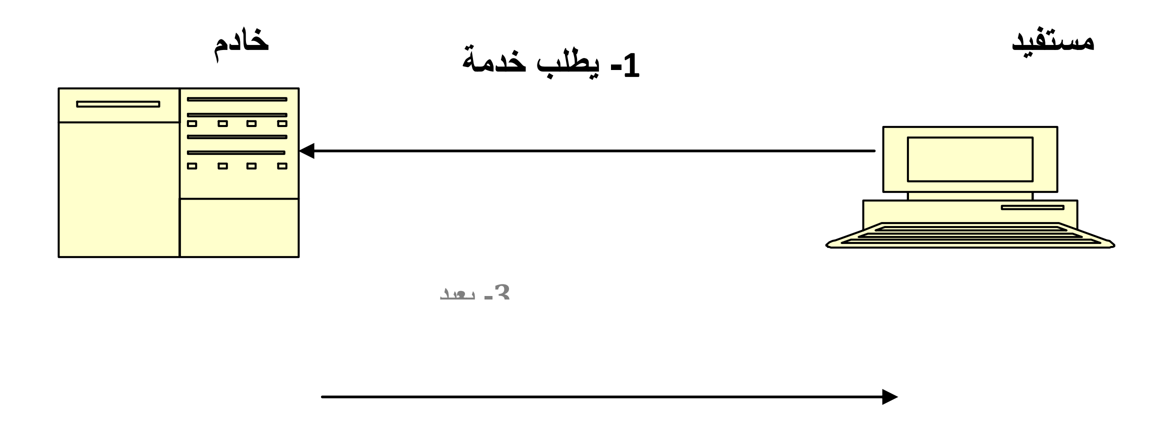
تسمح شبكة الحاسبات بنقل المعلومات المتعددة الوسائط (بيانات، نص، صورة، رسم أو صوت) بين الحاسبات بدون اعتبار للمسافات، و تهدف الشبكات إلى:

1. المشاركة في الموارد المختلفة : المعدات المادية (طابعة، قرص صلب، معالج)، البرامج و النظم (نظم إدارة قواعد البيانات، برامج مكلفة) أو البيانات (ملفات، جداول أو صفحات الويب) حيث يمكن لكل حاسب في الشبكة أن يستفيد من معدات، برامج أو بيانات تقدمها حاسبات أخرى.
2. الحصول على بيانات و معلومات من قواعد بيانات و بنوك معلومات في أماكن بعيدة.
3. نقل البيانات، المعلومات و البريد الإلكتروني من مقدمي الخدمات و توزيعها على المستفيدين في أماكن مختلفة و بعيدة.
4. نقل البريد الآلي من مقدمي خدمات الحاسبات الخادمة البريد و توزيعها علي الحاسبات المستفيدة(المشتركين) في أماكن مختلفة و بعيدة المسافات.
5. الاعتماد على حاسبات أخرى في حالة حدوث عطل أو خلل في حاسب ما.
6. سرعة إنجاز تنفيذ عمليات معقدة (تطبيقات رياضيات، محاكاة أو بحوث عمليات) بمشاركة أكثر من حاسب أو معالج في تنفيذ العمليات المطلوبة.

3.1. هيكلة الربط: نموذج الخادم/المستفيد Client/Server Model

نموذج الخادم/المستفيد هو الهيكلة المستعملة حاليا لربط حاسب بحاسب أخر عبر الشبكة. ويكون فيها المستفيد (Client) برنامج أو جهاز (طرفية، حاسب شخصي أو أي نوع من أنواع الحاسبات) يحتاج خدمة مقدمة من طرف برنامج أو حاسب أخر يسمي الخادم (Server)، والخدمات المقدمة من الحاسب الخادم تتلاءم مع أهداف الشبكة مثلا خدمة طباعة، خدمة ملفات، خدمة صفحات متعددة الوسائط، خدمة بريد إلكتروني الخ...

و تكون الهيكلة على الشكل التالي:



2- ينفذ الخدمة **4- يكمل العمل**

الشكل(2.1): هيكل نموذج الخادم/المستفيد

الجدول التالي يبين بعض الخدمات و اسم الخادم لكل خدمة

نوع الخدمة	اسم الخادم
طباعة	خادم طباعة / Printer Server
ملفات	خادم ملفات / File Server
صفحات	خادم صفحات / Web Server
بريد إلكتروني	خادم بريد إلكتروني / E-mail Server
شبكة	خادم الشبكة أو ملقم الشبكة / Network

خادم الشبكة أو ملقم الشبكة (Network Server) مثلا يقوم بإدارة و تنظيم مهام الشبكة و يوجد به نظام تشغيل الشبكة (NOS : Network Operating System).

ملاحظة: يمكن وجود أكثر من خادم في نفس الشبكة مهما يكون نوعها.

4.1. المكونات الرئيسية لشبكات الحاسبات

تتكون الشبكة من مكونات مادية و برمجيات، وتنقسم المكونات المادية إلى ثلاثة أنواع : الحاسبات (Computers) بشتى أنواعها، الكروت و الوسائط (Media) و الأجهزة الملحقة (Devices)، أما البرامج فتنقسم إلى برامج نظم تشغيل الشبكة، برتوكولات الاتصال و نظم إدارة الشبكة [4].

1.4.1.البرمجيات (Software)

تشمل البرمجيات عدة أنواع من بينها:

أ- نظم تشغيل الشبكة (NOS (Network Operating Systems

تتحكم نظم تشغيل الشبكة في كل المكونات المادية للشبكة و التنسيق بينها و تنظم طريقة الاستفادة منها ونظام Windows NT هو مثال من هذه الأنظمة.

ب- البروتوكولات(ومداولات) الاتصال Communication Protocols

تسمح البروتوكولات بتبادل البيانات و المعلومات بين الحاسبات المرتبطة بالشبكة، تتنوع البروتوكولات حسب تنوع الشبكات و البيانات و المعلومات المتبادلة. فشبكة الانترنت تستعمل مجموعة بروتوكولات معروفة باسم (TCP/IP (Transmission Control Protocol/Internet Protocol

وهناك بروتوكول لتبادل الملفات و يسمى (FTP (File Transfer Protocol

كما يوجد كذلك بروتوكول لتوصيل النصوص المتشعبة و المعلومات المتعددة الوسائط و يسمى HTTP (Hyper Text Transfer Protocol)

ج-نظم إدارة الشبكة Network Management Systems

تسمح نظم إدارة الشبكة بإدارة و توجيه الشبكة بطريقة ملائمة و التنبؤ بالمشاكل التي يمكن أن تحدث و إيجاد الحلول لها.

5.1.أنواع الشبكات

تتنوع شبكات الحاسبات من جوانب مختلفة سواء من ناحية أسلوب ربط المكونات مع بعضها البعض أو التغطية الجغرافية أو الوسائط المستعملة أو تطبيقاتها و استخدامها.

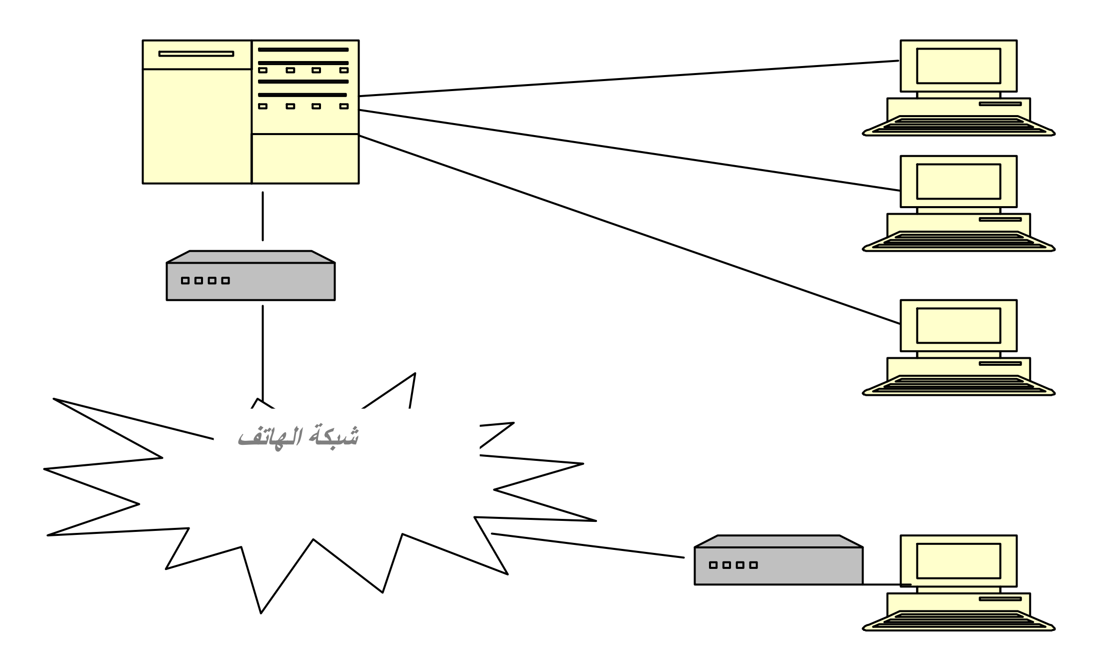
1.5.1.أساليب التوصيل

أساليب الربط تعبر عن كيفية ربط الحاسبات بعضها بعض على أساس نموذج الخادم/المستفيد.

ا- شبكات اتصال أحادية النقاط Point-to-Point Communications

يتم فيها اتصال مستفيد (حاسب شخصي أو طرفية) بالخادم البعيد (حاسب رئيسي) عن طريق وصلة مخصصة لها، يمكن أن تكون هذه الوصلة دائمة (و تكون خط مباشر مستأجر من شركة اتصالات من المستفيد إلى الخادم) أو مؤقتة (وتكون عن طريق شبكة الهاتف).

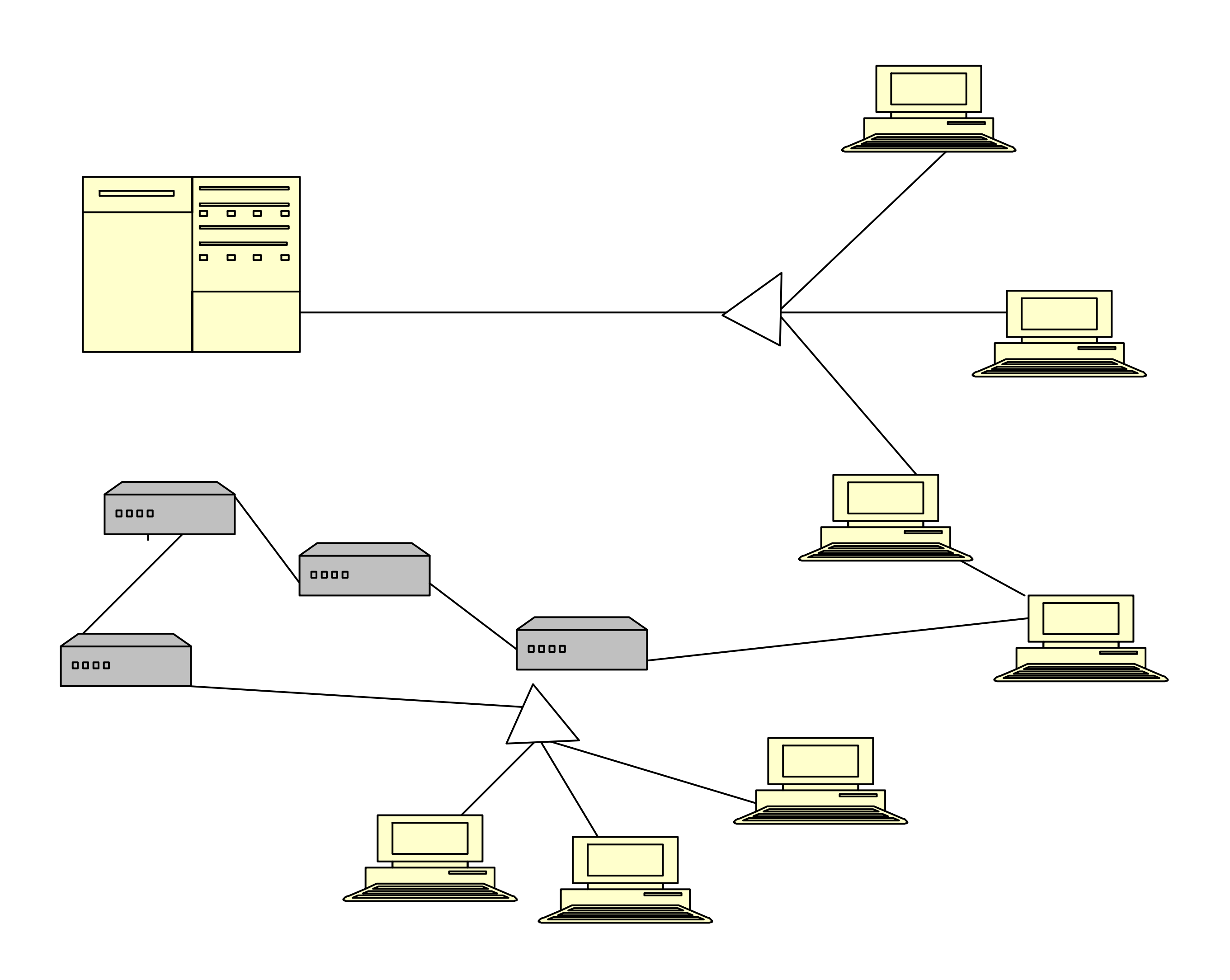
يتميز هذا النوع بإمكانية وجود اتصال مباشر بين المستفيد و الخادم في جميع الأوقات إلا أن بعض الخطوط يمكن أن لا تستغل كليا و يعتبر هذا هدر للموارد.



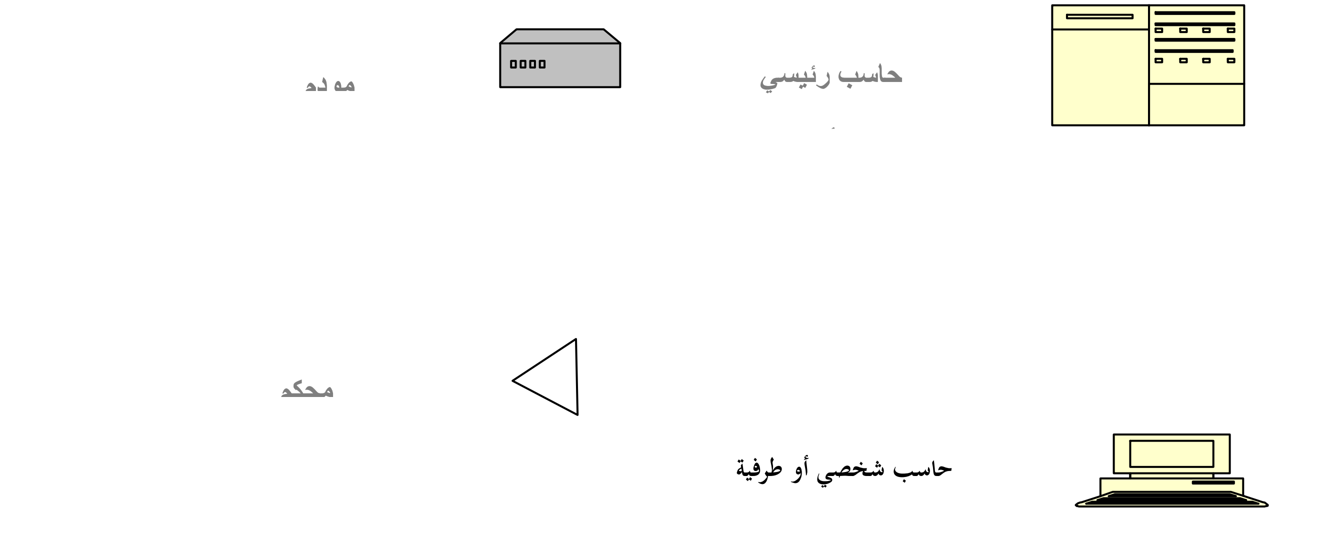
شكل(3.1): شبكة اتصال أحادية النقاط

ب- شبكات اتصال متعددة النقاط Multi-Point Communications

عند وجود إمكانية تجميع جغرافي لعدة حاسبات مستفيدة حيث أنها تشارك في نفس الوسيط الذي يربطها بالحاسب الرئيس أو الخادم فيسمى هذا الأسلوب بالمتعدد النقاط و يكون أكثر اقتصاد إلى الموارد لكنه يتطلب و جود محكم مع مبرمج لتشغيل وتيسير لكل جهاز إرسال و استقبال بياناته، و يوضح الشكل التالي شبكة اتصال متعددة النقاط.



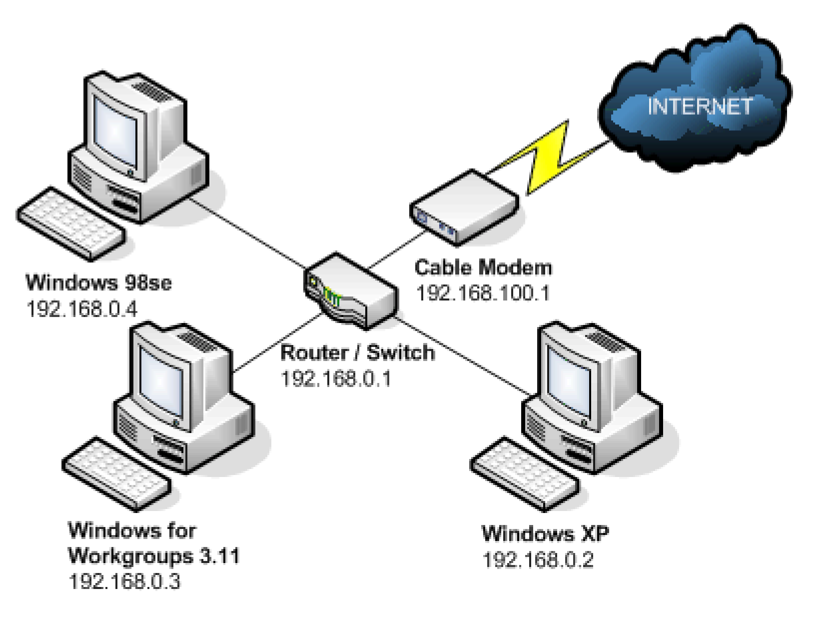
شكل(4.1): شبكة اتصال متعددة النقاط



2.5.1.أنواع الشبكات من حيث التغطية الجغرافية

يمكن تقسيم شبكات الحاسبات من حيث التغطية الجغرافية إلى ثلاثة أنواع : الشبكات المحلية، الشبكات الإقليمية و الشبكات الواسعة.

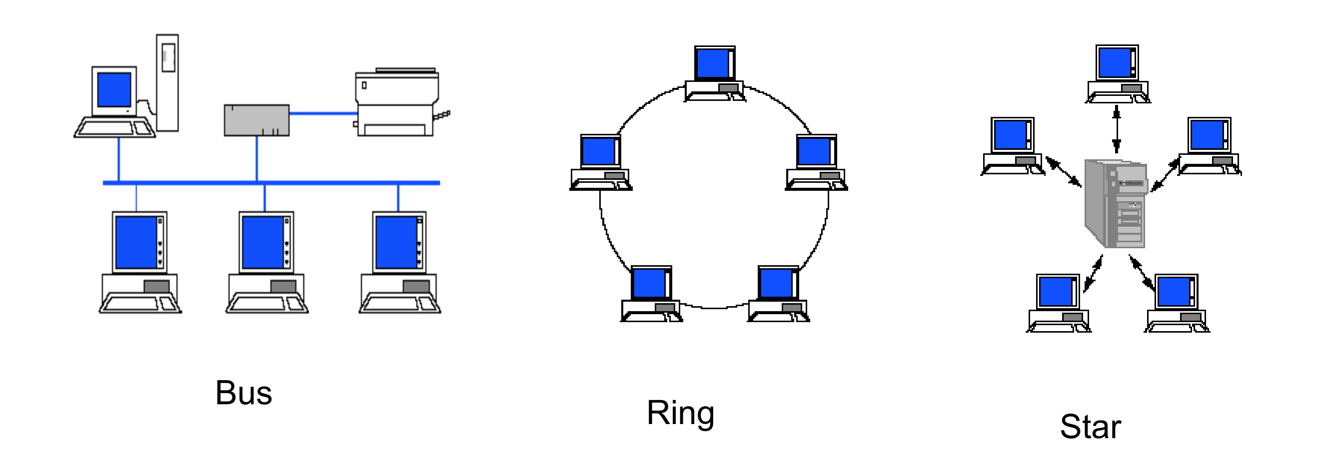
أ- شبكات الحاسبات المحلية (LAN (Local Area Network



شكل(5.1):الشبكات المحلية

الشبكات المحلية تتميز بكونها محدودة جدا في المسافات (لا تتجاوز بعض الكيلومترات) بين الحاسبات التي تربطها أو كونها كذلك مملوكة من مؤسسة ما. إلا انه يمكن ربط عدة شبكات محلية في أماكن وذات استعمالات مختلفة ببعضها البعض بواسطة أجهزة ملحقة (مثل العبارات أو مسارات الربط).

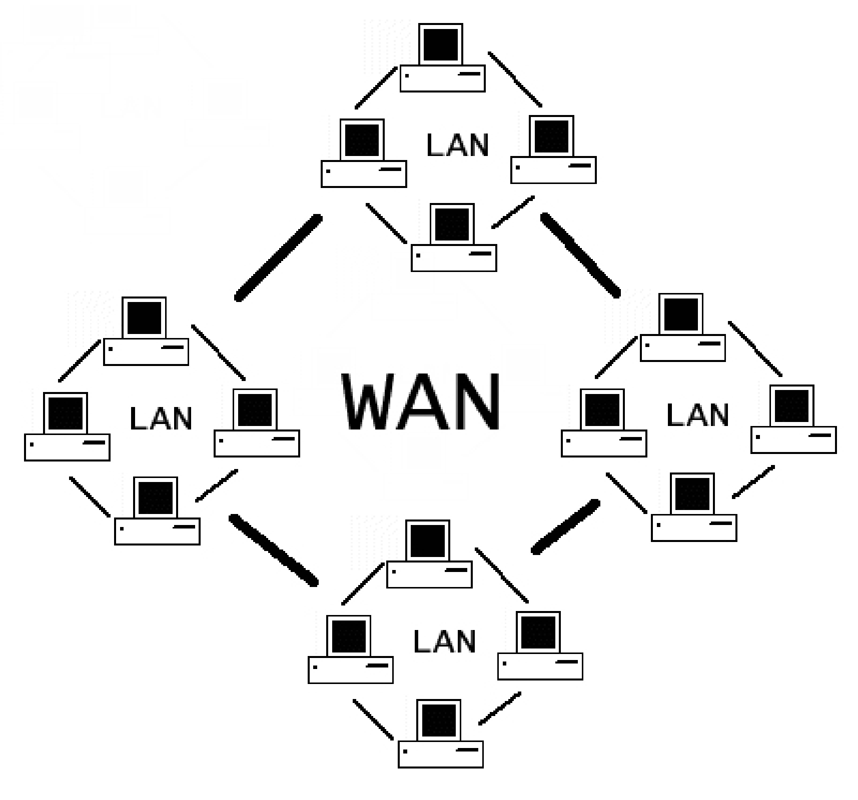
تتميز شبكة الحاسبات المحلية بسرعتها الفائقة لنقل البيانات التي تتراوح بين 10 إلى 100 أو 1000 ميجا بت في الثانية للشبكات العالية السرعة (10 to 100 or 1000 Mbps) حسب الوسيط و التقنيات المستعملة (كوابل محورية، أسلاك مبرومة أو ألياف ضوئية).الشكل رقم 6 يبين ثلاثة بنيات مختلفة (بنية المسار المشترك : Bus Topology، البنية النجمية : Star Topology والبنية الحلقية Ring Topology).



الشكل(6.1):بنيات مختلفة لتقنيات الشبكات

ملاحظة: يمكن إنشاء شبكة محلية باستخدام تقنية واحدة أو دمج أي عدد من التقنيات المذكورة سابقا في الشكل (6.1).

ب-شبكات الحاسبات الواسعة WAN (Wide Area Network)



شكل(7.1): شكل الشبكات الواسعة

تشمل الشبكات الواسعة كل أنواع الشبكات المستخدمة في نقل البيانات و المعلومات من أماكن بعيدة و في مساحة جغرافية واسعة (من عدة كيلومترات إلى آلاف الكيلومترات)، و تستخدم فيها كل أساليب الاتصال السابق ذكرها، و تحتوي الشبكة الواسعة على عدد كبير جدا من الطرفيات و الحاسبات.

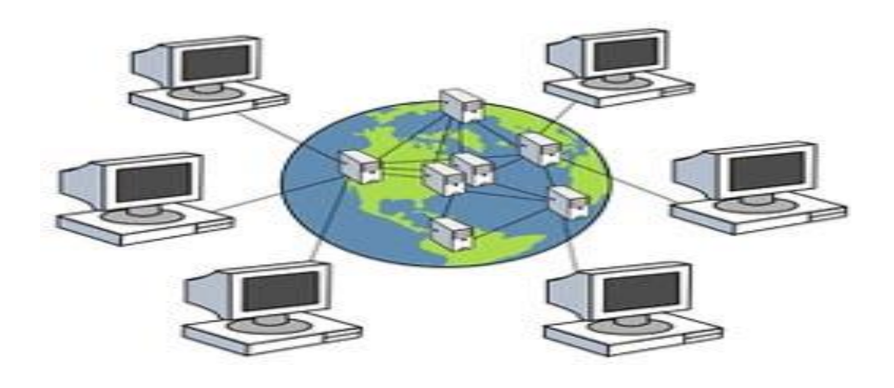
سرعة الشبكات الواسعة ضعيفة مقارنة بالشبكات المحلية حيث أنها غالبا ما تعتمد على شبكة الهاتف و مجموعة كبيرة من أجهزة ملحقة من أهمها المودم (Modem) ذو السرعة المنخفضة التي تقاس بالكيلو بت في الثانية (x Kbps) بينما تقاس سرعة الشبكات المحلية بالميجا بت في الثانية (x Mbps).

يوجد مثلا مؤسسات كبيرة كشركات الطيران تستعمل الشبكات الواسعة حيث أن مكاتبها موزعة في كل أنحاء العالم.



الشكل(8.1) محول (Modem) خارجي

ج-شبكات الحاسبات الإقليمية(MAN (Metropolitan Area Network



شكل(9.1):الشبكات الإقليمية

تستخدم الشبكات الإقليمية في مساحات جغرافية متوسطة نسبيا تصل إلى عدة كيلومترات و تستعمل في ربط حاسبات موجودة في نفس المدينة أو مجموعة قريبة من المدن.

1.6. مفاهيم حول النموذج المرجعي OSI

اختصار ل (Open Systems Interconnection Basic Reference Model) المرجع وضعته المنظمة الدولية للمعايير (International Standards Organization(ISO سنة1983،رقم 7498الخاص بتصميم الشبكات .ويحدد هذا النموذج كيفية تخاطب بروتوكولات ومعدات الشبكات وكيفية عملها معا، هذا الطراز المرجعي reference model الذي حددته المنظمة، يقسم الاتصالات بين كل حاسب وآخر إلى سبع طبقاتlayers، ليكون نموذج نظري وقاعدي لتصاميم بروتوكولات الاتصالات بين الشبكات الحاسوبية[1][12].

1.6.1.مهامه

وظائف الاتصال والتنظيم حسب مرجع OSI مقسمة على سبع طبقات (Layers) مختلفة. لكل طبقة دور يضم مجموعة مهمات يتطلب تحقيقها داخلها وعبر التواصل مع الطبقة التي تسبقها أو التي تليها حسب الترتيب. ويشرح مرجع OSI ذلك من خلال 4 أجزاء هي:

1. النموذج القاعدي
2. نظام الحماية
3. التسمية والعنونة
4. الإطار العام للتسيير(Routing)

تم مراجعة المرجع سنة 1994 بتركيز على الجزء الأول.

يوصف المرجع على أنه نظري، ذلك أن المرجع يصف بشكل عام المهام والأدوار التي تقوم بها أنظمة الربط الشبكية من دون الدخول في التفاصيل التقنية أو ذكر للتكنولوجيات المستعملة، بعض تفصيل المرجع من حيث العمليات والوظائف لم يتم لحد الآن دمجها في أحد من الأنظمة[12].

2.6.1.أهدافه

1. ضمان نقل البيانات عبر الشبكة بطريقة آمنة وسليمة.
2. توفير نفقات عرض الحزمة الدولي.
3. توفير جودة أفضل لخدمة نقل الصوت عبر بروتوكول الإنترنت.VoIP
4. إدارة الخدمة وتوسّع الشبكة.

طبقات المرجع



الشكل (10.1) الطبقات السبع

يعرض مرجع (OSI) على شكل 7 طبقات (التي تكونه) بشكل عمودي، أعلاه الطبقة السابعة وأسفله الطبقة الأولى. [5]

3.6.1.وظائف الطبقات:

1. الطبقة الفيزيائية أوطبقة المكونات الماديةPhysical layer

هذه الطبقة مسؤولة عن انسياب البيانات عبر وسائط الاتصال، فهي تتعامل مع البيانات التي تكون في شكل بتات bits ترسلها الطبقة المادية Physical layer الموجودة بمصدر الإرسال كما تستقبلها الطبقة الماديةPhysical layer بالجهاز المستقبل.

2. طبقة ربط البيانات Data link layer

عند تلقي البيانات من الطبقة المادية، تقوم طبقة ربط البيانات بالتحقق من صحة وكفاءة تدفق وانسياب البيانات من الطبقة المادية، كما تتحقق من عدم وجود أخطاء، ثم تغلف البتات bits في إطارات frames [1].

Data Link Frame
Data bits
Destination address | Source address | Other header | ...1001101010001001... | Frame footer

3. طبقة الشبكةNetwork layer

هذه الطبقة تحدد بروتوكولات تمرير البيانات data routing لضمان وصول المعلومات من محطة لأخرى على الشبكة. فعند وصول البيانات لطبقة الشبكة، فإن عنوان مصدر وعنوان وجهة البيانات التي يحتويها كل إطار frame يتم فحصه لتحديد إذا ما كانت البيانات قد وصلت إلى الوجهة النهائية [1].

4. طبقة النقلTransport layer

هذه الطبقة تهيئ تمرير البيانات بين الأنظمة أو المضيفات hosts وتحدد بنية الرسالة message structure، كما تشرف على صحة الإرسال، وذلك بإجراء بعض العمليات لمراجعة الأخطاء[1].

5. طبقة التحاور Session layer

هذه الطبقة تنسق الاتصالات وتحافظ على مقومات الجلسة طول مدة استخدام النظام كما تبدأ وتنهي الاتصالات بين التطبيقات، حيث تقوم بتأمين وتسجيل العميل logging، وبعض العمليات الإدارية الأخرى [1].

6. طبقة التقديم Presentation layer

تحدد هذه الطبقة كيفية تهيئة البيانات، وعرضها، وتغييرها، وفك أكوادها عن طريق الترجمة من صيغة التطبيق إلى صيغة الشبكة، وبالعكس. وهذه الطبقة مهمتها تهيئة المعلومات التي ترسلها طبقة التطبيقات Application layer [1].

7. طبقة التطبيقات Application layer

هذه هي الطبقة العليا في نموذج وصل الأنظمة المفتوحة، وهذه الطبقة توفر خدمات الشبكة للمستفيد النهائي وهي تستفيد من الطبقات التي تحتها ولكنها معزولة تماما عن تفاصيل المعدات والأجهزة، وتتعامل هذه الطبقة مع البيانات المرسلة إلى والواردة من الطبقة السادسة بالنموذج، وهي طبقة التمثيلPresentation layer، حيث تحدد الطريقة التي تتفاعل بها البرامج التطبيقية application programs مع الشبكة، فهي تقدم خدمات التطبيقات مثل خدمة انتقال الملفات، والبريد الإلكتروني، وإدارة قواعد البيانات، وبرامج محاكاة الطرفيات terminal emulation، وأي خدمات تقدمها برامج الشبكة، وخدمات الشبكة في هذه الطبقة تكون عادة بروتوكولات تتعامل مع بيانات المستفيد والتطبيقات HTTP،Telnet،SMTP، FTP هي تطبيقات توجد في هذه الطبقة،فمثلا، في حالة التطبيق المتعلق بمتصفح الويب Web browser، فإن بروتوكول طبقة التطبيقات HTTP، يغلف البيانات المطلوبة لإرسال واستقبال محتويات صفحة الويبWeb page.

ومن البروتوكولات التي تعمل في طبقة التطبيقات:

(HTTP) Hyper Text Transfer Protocol

يؤمن تصفح صفحات الويب عن طريق تأمين تناقل المعطيات بين مخدم الويب web server ومتصفح الويب web browser[12].

(FTP) File Transfer Protocol

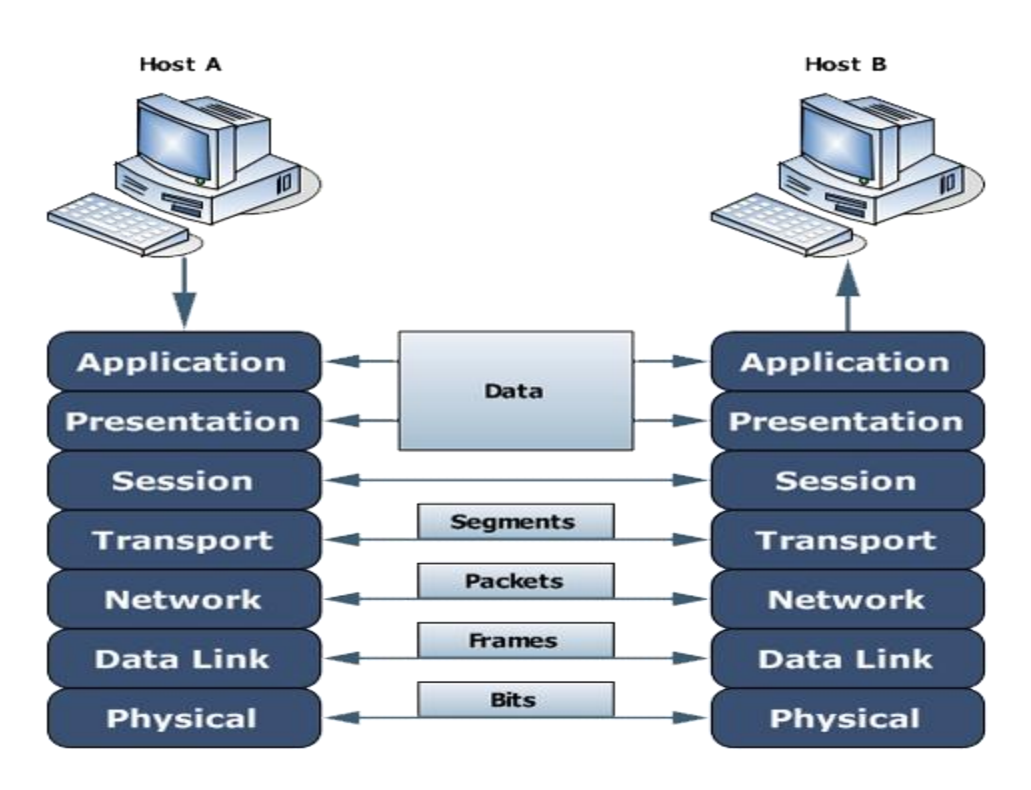
يؤمن تناقل الملفات عبر الشبكة[12].

(SMTP) Simple Mail Transfer Protocol

يؤمن تراسل البريد الإلكتروني عبر الشبكة[12].

SNMP، DNS،TELNET

ومن الملاحظ أن تطبيقات المستخدم النهائية لا تعمل ضمن طبقة التطبيقات فمتصفح الويب مثلا ليس من طبقة التطبيقات ولكنه يستخدم البروتوكول HTTP الذي ينتمي إلى طبقة التطبيقات من أجل التخاطب مع مخدم الويب[13].



كيفية عمل الطبقات السبعة حسب الشكل(11.1)

يقوم الحاسب A بتحضير البيانات لإرسالها إلى الطرف B المستقبل حيث تصل البيانات بالطبقة المكافئة لها و ذلك لأن المستويات تتحدث نفس اللغة.

يقوم الحاسب A ببدء الإرسال في القمة و نزولاً باتجاه الطبقة الفيزيائية وعندما تمر الرزمة من مستوى إلى أخر يقوم كل مستوى بإضافة معلومات العنونة و التنسيق الخاصة بها.

عندما تمر الرزمة عبر وسط النقل يتم الاتصال بين الحاسبين عن طريق هذه الطبقة .

تقوم الطبقة الفيزيائية في الجهاز B المستقبل بتحويل الدفق التسلسلي من البتات إلى رزم .

تقوم كل طبقه بأخذ معلومات العنونة و التنسيقات التي قامت بإضافتها سابقاً.

الفصـــــــــل الثانـي

مخاطر الشبكات و طرق حماية المعلومات داخل الشبكات

الفصـــــــل الثاني: التأمين والطرق المختلفة لحماية المعلومات داخل الشبكات

1.2 ما هو الأمن ؟

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات، قد نتكلم مثلاً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات، لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن[11].

بناء على ذلك فقد قمنا بصياغة مصطلح "أمن الشبكات" ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات، تقوم هذه الوحدة بتعريف أمن الشبكات ضمن سياق أمن المعلومات، أي أننا عندما نتحدث عن أمن الشبكات فإننا نعني أمن المعلومات في الشبكات.

2.2. أمن المعلومات Information security

لكي نتمكن من استيعاب مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم، لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً باسم أمن الاتصالات Communication Security (COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات"[11].

تضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security، كما تضمّن تعريف أمن الإتصالات خاصيتين تتعلقان بموضوع هذه الوحدة: السرية والتحقق من الهوية.

أمن المعلومات = سريّة + سلامة + توفر + تحقّق

يمكن أن يكون هناك أمن من دون معلومات سرية، وهذا يضمن عدم اعتراض أن المستخدمين غير المصرح لهم، لا يستطيعون نسخ المعلومات،في الوقت نفسه، السلامة ضرورية جدا حيث يجب أن يكون للمنظمات ما يكفي من الثقة في دقة المعلومات التي تعمل عليها،علاوة على ذلك، أمن المعلومات يتطلب من المنظمات أن تكون قادرة على استرجاع البيانات، والتدابير الأمنية لا قيمة لها إذا كانت المنظمات لا يمكنها الوصول إلى المعلومات الحيوية التي يحتاجونها للعمل عليها .أخيرا، المعلومات غير آمنة دون المصادقة عليها تحديد ما إذا كان يؤذن للمستخدم النهائي في الوصول [7].

3.2.أمن الشبكات Networks Security

تعرّف توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي:

"حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات"[11].

1.3.2. تطبيق الخصائص الأمنية

يقدم النموذج المرجعي OSI مبدأ "التكديس Stack". إن استخدام نموذج للبروتوكولات يعمل وفق مبدأ الطبقات أو التكديس يعني أن كل طبقة ستستخدم وظائف الطبقة الأدنى منها فقط في حين تقوم بتخديم الطبقة التي تعلوها مباشرة فقط، ينعكس أسلوب التصميم وفق مبدأ الطبقات بشكل مباشر على كيفية تطبيق الخصائص الأمنية.

4.2 أهداف امن الشبكات

يتضمن مفهوم أمن الشبكات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الإنكار.

السرية Privacy or Confidentiality :

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص).

بحيث لا يطلع على المعلومات إلا الأطراف المسموح لها بذلك، وللحفاظ على الخصوصية،لابد من التحكم بعملية الولوج، وأكثر طرق التحكم انتشارا هي:استخدام كلمات المرور Passwords، والجدار الناري Firewall، إضافة إلى شهادات الترخيص Authorization Certificates[8].

التحقق من الهوية Authentication:

إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عملية التزوير وانتحال الشخصية)[8].

التكامل Integrity:

تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بناء المعلومات مع البيانات المخزنة.

لابد من حماية عمليتي نقل المعلومات وتخزينها، وذالك لمنع أي تغيير للمحتوى بشكل متعمد أو غير متعمد، وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام [8].

التوفر Availability :

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.

<u>مكافحة الإنكار (المسؤولية) Non-repudiation:</u>

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات[6].

آليات معينة للحماية من إنكار المسؤولية: التشفير، التوقيع الالكتروني، التحكم بالوصول، سلامة البيانات، تبادل الصلاحيات، المرور الزائد، التحكم بالمسار، الشهادة القانونية.

-آليات بينية للحماية (وسطية):

الوظيفية الموثوقة، أغلفة الحماية، كشف الأحداث، ممرات تدقيق الحماية، إصلاح الحماية(الخلل)[6].

5.2.المخاطر التي تتعرض لها الشبكات:

تحدث المشكلة الأمنية عندما يتم اختراق النظام من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة، وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت،حيث يتسبب الاختراق في مشاكل مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة، ويمكن أن يتعذر الدخول إلى البيانات، يمكن اختراق المعلومات الشخصية للمستخدم.

وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة، فمن الممكن أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام.

كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات تستهدف إبطاء أو شل حركة مرور البيانات عبر الشبكة، إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة[10].

1.5.2 فيروسات الشبكات Network Viruses

لقد ارتبط ظهور الفيروسات بانتشار مفهوم الشبكات مثل شبكة الانترنت، حيث استخدام البريد الالكتروني ساهم في نشر هذه الفيروسات وخصوصا الرسائل التي تأتي لاحقا (Attachment) ومن أشهر الفيروسات ما يلي:

1.1.5.2 ديدان Worms

الديدان هي برامج الكمبيوتر التي تكرر نفسها عبر وصلات الشبكة، دون تعديل أو ربط نفسها ببرنامج مضيف، يعتبر بعض الخبراء أن الديدان نوع خاص من الفيروسات بدلا من منحها فئة خاصة بها، إلا أن التصنيفات توضح أنها ديدان منفصلة تقليديا عن الفيروسات. ويمكن أيضا أن العديد من المتغيرات الأكثر حداثة التي تم وصفها عموما باسم الديدان، وتصنف على أنها فيروسات أو دودة / فيروسات هجينة[10][15].

أمثله عن الديدان:

W32/Klez: ومغايراتها و هي تنتقل عن طريق ملحقات الإيميل.

W32Lovesan.worm و هي تنتقل عند استخدام الانترنت عبر وصلات TCP و UDP غير محمية الأعراض هي تتضمن أي شيء, من رسائل الإزعاج إلى الملفات المعطوبة [22].

إن الدودة المضيفة (Host Worm) تستخدم الشبكة لنسخ نفسها فقط على أجهزة الكمبيوتر المتصلة بالشبكة، بينما توزع الدودة الشبكية (network worm) أجزاءها على عدة كمبيوترات وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء، ويمكن أن تظهر الدودة على أجهزة حواسيب منفصلة، فتنسخ نفسها إلى أماكن متعددة على القرص الصلب .

إن الضرر الأساسي التي تتسبب به الدودة هو إبطاء سرعة عمل الشبكات.

2.1.5.2 حصان طروادة Trojans

أحصنة طروادة هي البرامج التي تدعي أنها شيء واحد (تظهر عادة غير ضارة)، ولكن تنقل حمولة غير مرغوب فيها ومدمرة في كثير من الأحيان، تماما مثل الحصان الخشبي الأصلي، وأحصنة طروادة هي وسيلة لإيصال أشكال أخرى من البرامج الضارة وغالبا ما تعتمد على قليل من الهندسة الاجتماعية لخداع المستخدم في إطلاق هذا البرنامج في الواقع. على الرغم من الاتجاه السائد للمستخدمين تغطية وسائل الإعلام و تحذيراتها لا تكفي حيث عند النقر على مرفقات البريد الإلكتروني (وخاصة التنفيذية)، وطروادة لا يزال أداة فعالة لنشر البرمجيات الخبيثة، في الماضي والحاضر، واعتبرت برامج حصان طروادة "خبيثة " لأنها ببساطة أطلقت حمولتها التي كان عليها، التغيرات الحديثة لطمس هذا التمييز، وتستخدم لإطلاق الديدان الهجينة / فيروسات التي يمكن أن تطغى على الشركات بسرعة بسبب أنظمة البريد الإلكتروني[15].

أمثله عن أحصنة طروادة، أو التروجانات:

JS/NoClose :

والتي تشغل روتين الجافا سكريبت لتولد تطبيقات أو صفحات HTML لا يستطيع المخدم إغلاقها[22].

Helvis:

و هذا النوع يجمع كل الإيميلات الصادرة و الواردة من إيميل المستخدم الشخصي و يقوم بإرسال هذه الإيميلات إلى عنوان الشخص الذي صمم الفيروس[22].

2.5.2 البرمجيات الخبيثة Malware

كما ذكر سابقا، الفيروسات، والديدان، وأحصنة طروادة ليست هي الشكل الوحيد من أشكال البرمجيات الخبيثة. وهناك عدد من المنظمات غير تكرار أشكال البرمجيات الخبيثة التي تهدف إلى تدمير أو سرقة البيانات، وتجعل النظم مفتوحة ، وتعطل الشبكات، أو خطف الأنظمة البعيدة، وتستخدم العديد من البتات من البرامج الضارة مثل الحمولة لبرنامج حصان طروادة، ولكن يمكن أيضا أن توزع يدويا من قبل الأفراد مع إمكانية الوصول الفعلي إلى جهاز الكمبيوتر أو الشبكة، أو إدراجها في جهاز كمبيوتر غير محمي الذي يعمل مع اتصال إنترنت[15].

- **الهجمات الإغراقية الموزعة (DDoS Agents)**

الحرمان من الخدمة محاولات تطغى على موارد الشبكة أو النظام من أجل منع المستخدمين من الوصول إلى هذه الموارد، من أجل تحقيق هذا الهدف على هدف كبير (مثل موقع التيار)، قراصنة النظم يستعملون وسائل لمساعدتهم في هجماتهم عن طريق إرسال برامج حصان طروادة التي تثبيت على جهاز الكمبيوتر المصاب، تكمن هذه العوامل نسبيا حتى حصولهم على مزيد من التعليمات من جهاز الكمبيوتر الخاص بالهاكر (عادة ما تكون التعليمات البرمجية صغيرة جدا)، ومن ثم تبدأ الفيضانات في الشبكة (أو هدف محدد) مع حركة المرور ونقل البيانات[15].

- **القنابل المنطقية (Logic Bombs)**

وهذا النوع من البرامج الضارة ينتظر ضغط زر محدد (مثل تاريخ أو تسلسل الأحداث) لإطلاق الفيروسات، وكان أسلوب شائع من كتاب الفيروسات لعدة سنوات. للقراصنة والموظفين الساخطين، هو وسيلة فعالة لإيصال حمولة مدمرة لفترة طويلة بعد مغادرة وتنظيف المسارات، ودفن برنامج على خادم الشركة في التحقق من وجود حساب مستخدم له، إذا تم حذف حسابه أو تعطيله، فإنه يتم إطلاق برنامج والبدء في حذف الملفات على خوادم الشبكة. لسوء الحظ هذا النوع من القنابل المنطقية عادة ما يكون برنامج مخصص أو نصي حيث يصعب اكتشافه، ولا يتم تحديده بواسطة برامج مكافحة الفيروسات[15]

- **الألغام (Mines)**

مثل الألغام العسكرية المادية، ويمكن وضع البرامج الخبيثة على ملقم ملفات أو وضعها على أقراص الأبرياء بحيث يتم تركها في الخادم. وعادة ما تكون هذه البرامج المخصصة تكتب وتنشر من قبل الموظفين الساخطين أو الهاكر، ويكاد يكون من المستحيل الدفاع ضدها. كما يمكن أن يدفع الفضول لإغراء المستخدم أو المسؤول لفتحها. يمكنك الحماية ضد التهديدات القائمة على القرص عن طريق تعطيل التشغيل التلقائي لمحرك الأقراص المضغوطة على محطات العمل و الخوادم، فضلا عن القدرة على التمهيد من قرص مرن[15].

- **كلمة السر واللصوص (Password Stealers and Keystroke Loggers)**

هناك عدد من برامج الطرف الثالث والتي تمت كتابتها لالتقاط ضربات المفاتيح للمستخدمين، وكتابة البيانات إلى السجل ومن ثم إرسال السجل إلى مكان بعيد أو عنوان البريد الإلكتروني. هذه غالبا ما تكون صعبة لتحديد مكان الإصابة، وربما لا يمكن الكشف عنها بواسطة برنامج مكافحة الفيروسات.

ويتم تعبئتها مع بعض البرامج التجريبية، برامج مجانية، وأدوات مع برامج إضافية، ويمكنها مراقبة عادات التصفح الخاصة بك، وبيع حتى وقت وحدة المعالجة المركزية غير المستخدمة و المساحة غير المستخدمة من القرص إلى الشركات الأخرى التي تستهلك في هذه العملية أيضا موارد الشبكة الخاصة بك، وبطبيعة الحال يتم دفن الأدوات القانونية التي تسمح لهؤلاء الباعة للقيام بذلك في اتفاقية ترخيص المستخدم النهائي أن لا أحد يقرأ ذلك [15].

- **أدوات الوصول (RAT) Remote Access Tools**

المعروف أيضا باسم "وكلاء مستترين"، وهذه الأدوات تعطي المتسللين وسيلة الدخول إلى نظام موثوق به موجود على الشبكة. في فئة البرمجيات الخبيثة، ونحن لا نتحدث عن المنتجات الشعبية مثل برنامج Laplink أو برنامج PCAnywhere (على الرغم من أنها يمكن أن تشكل خطرا على الأمن إذا لم يتم تكوينها بشكل صحيح)، ولكن البرامج التي يتم تفعيلها كلما تم تشغيل الكمبيوتر وتعمل في صمت في الخلفية دون معرفة المالك. وبالإضافة إلى ذلك، فإن هذه البرامج كثيرا ما يخطر الكمبيوتر المسيطر عندما تكون نشطة، تقديم معلومات عن العمليات الجارية، والسماح لمتسلل لتثبيت برامج ضارة أخرى مثل كلمة السر stealers.[15]

البرامج غير المرخصة (Unlicensed software)

إذا كنت تعتقد أن تفشي الفيروس أمر غير مكلف، في البرامج الغير المرخصة. في حين ليس من الناحية الفنية "الخبيثة" لأنها ليست ضارة حسب التصميم، والبرمجيات غير المرخصة أو المقرصنة يمكن أن تكلف الشركة 20000 $ لكل حادث إذا تم تدقيقها في أي وقت من الشركة، وقد أفلست بعض الشركات بسببها، حيث يتم تشغيل معظم عمليات مراجعة الحسابات بواسطة مكالمات هاتفية من الموظفين السابقين

الساخطين، يمكن للشركة أن لا تستطيع تجاهل هذا التهديد، وتكمن في برامج مجانية وبرنامج كومبيوتري حيث تحطم أنظمة التشغيل والشبكات مع حركة المرور غير المرغوب فيها، إلا إذا كنت تؤمن محطات العمل الخاصة بالشركة ومراجعتها بانتظام، قد لا تعرف أبدا ما يقوم المستخدمين بتثبيته على الشبكة حتى فوات الأوان، إنها ليست مجرد البرمجيات التي يمكن أن تكلف الشركة، يمكن أن ملفات MP3 أو غيرها من أشكال مواد محفوظة الحقوق التي يتم تخزينها على خوادم يؤدي إلى فرض غرامات صارمة، دفعت شركة RIAA، 1 مليون دولار في تسوية خارج المحكمة لاستضافة ملفات MP3 على خادم داخلي للموظفين فيها، الفيروسات يمكن لعدد قليل منها أن يسبب هذا القدر من الضرر في حين تبقى أساسا "لم يتم كشفها" على الشبكة[15]

3.5.2 الهاكر Hackers :

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي، وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة، غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

الهاكرمهتمّون جدا بأنظمة الحاسوب، مسرّات الهاكر تكمن في كسب فهم عميق عن طرق العمل الداخلي لشبكات الحاسوب وأنظمة الحاسوب بشكل خاص، الهاكر غير مؤذون عادة، بالرغم من أن العديد من الناس في أوقات يستعملون كلمة "الهاكر" للتعبير للإشارة إلى أن كلاهما جيد وسيئ (خبيث)[8].

4.5.2 لصوص الهوية piracy identity:

يستخدم للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم

المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول إلى الموقع، هناك برامج لمكافحة السرقة والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروفا و مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني[10].

6.2.الطرق المختلفة لحماية المعلومات داخل الشبكات

1.6.2.التشفير أو التعميةcryptography

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري، فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة، وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير، و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب، فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها، وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم، أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لارتباط العالم ببعضه عبر شبكات مفتوحة، وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات، فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات، ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

1.1.6.2. ما هو التشفير أو التعمية(Cryptography)

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات، التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة مثل الإنترنت وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل له، وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (Crypto analysis) هو علم لكسر و خرق الاتصالات الآمنة[14].

2.1.6.2.أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

السرية أو الخصوصية: (Confidentiality)

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها .

تكامل البيانات: (Integrity)

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

إثبات الهوية: (Authentication)

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم)

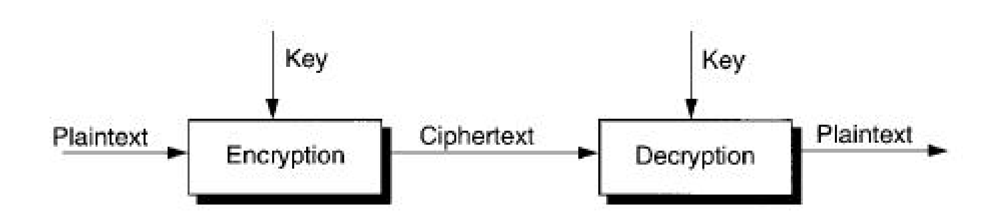
عدم الجحود:(Non-repudiation)

وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما[6].

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم

..3.1.6.2كيفية عمل التشفير:

خوارزمية التشفير هي دالة رياضية تستخدم في عملية التشفير وفك التشفير، وهي تعمل بالاتحاد مع المفتاح أو كلمة السر أو الرقم أو العبارة، لتشفير النصوص المقروءة، نفس النص المقروء يشفر إلى نصوص مشفرة مختلفة مع مفاتيح مختلفة، والأمن في البيانات المشفرة يعتمد على أمرين مهمين قوة خوارزمية التشفير وسرية المفتاح. فيما يلي رسم توضيحي صورة (1.2)



صورة(1.2) : طريقة عمل التشفير

.4.1.6.2أنواع التشفير:

حالياً يوجد نوعان من التشفير وهما كالتالي:

التشفير التقليدي (Conventional Cryptography)

تشفير المفتاح العام (Public Key Cryptography)

.1.4.1.6.2التشفير التقليدي:

يسمى أيضاً التشفير المتماثل (Cryptography Symmetric) وهو يستخدم مفتاح واحداً لعملية التشفير وفك التشفير للبيانات، ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم، حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات.

بعض الأمثلة على أنظمة التشفير التقليدي:

شفرة قيصر: وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها .المثال التالي يوضح طريقة عمل شفرة قيصر: إذا شفرنا كلمة "SECRET" واستخدمنا قيمة المفتاح 3، فإننا نقوم بتغيير مواضع الحروف ابتداءً من الحرف الثالث وهو الحرف "D"، وعليه فان ترتيب الحروف سوف يكون على الشكل التالي:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

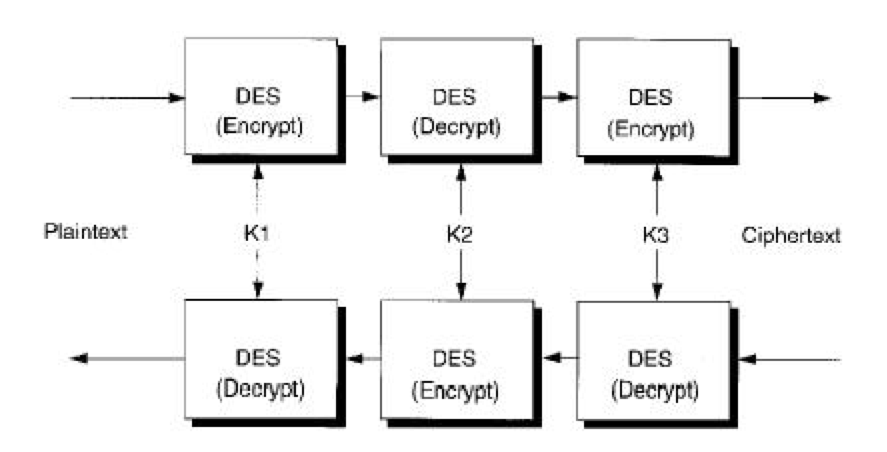
الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" تكون على الشكل الحالي:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

الآن قيمة الـ A à D، B à E، C à F، وهكذا.

بهذا الشكل فان كلمة "SECRET"سوف تكون "VHFUHW" لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة؛ يجب أن ترسل له قيمة المفتاح "3".

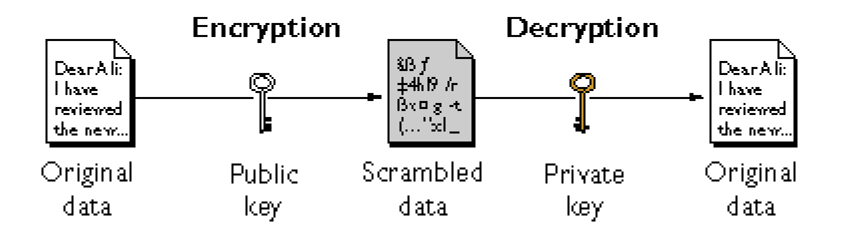
تشفير البيانات القياسي(DES): طُور هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الكمبيوتر وزيادة سرعة معالجته للبيانات، حيث أنه قد يتم كشف محتوى رسائل مشفرة به في وقت قصير[14].



شكل(2.2): تشفير DES

2.4.1.6.2.تشفير بالمفتاح العام:

أو ما يعرف بالتشفير اللامتماثل (Cryptography Asymmetric): تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاصPrivet key ، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل .المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص. فيما يلي رسم توضيحي صورة (3.2) .



صورة(3.2): توضح عمل التشفير باستخدام المفتاح العام والمفتاح الخاص

بعض الأمثلة على أنظمة تشفير المفتاح العام:

RSA، DSA،PGP

جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص.

مزايا وعيوب التشفير التقليدي والتشفير باستخدام المفتاح العام:

التشفير التقليدي أسرع بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه يستخدم مفتاح واحد فقط، فهو عرضة أكثر للاختراقات، أما تشفير المفتاح العام فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة للاختراقات، ولكنه أبطأ من التشفير التقليدي،ونتيجة لهذه المزايا والعيوب أصبحت الأنظمة الحديثة تستخدم كلا الطريقتين حيث أنها تستخدم الطريقة التقليدية للتشفير وأما تبادل المفتاح السري الواحد بين الأطراف المتراسلة تتم من خلال استخدام طريقة تشفير المفتاح العام[14].

قياس قوة التشفير:

التشفير قد يكون قوياً أو ضعيفاً، حيث أن مقياس القوة للتشفير هو الوقت والمصادر المتطلبة لعملية كشف النصوص غير مشفرة من النصوص المشفرة. نتيجة التشفير القوي هو نص مشفر يصعب كشفه مع الوقت أو توفر الأدوات اللازمة لذلك.

2.6.2.الشهادة الرقمية Digital Certification

تعريف الشهادة الرقمية :

"هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحويها جهاز الخادم (server) [10].

1.2.6.2. مفاهيم أساسية:

المفتاح الخاص

مفتاح سري يستخدمه صاحبه لفك تشفير الرسائل المرسلة له، وكذلك يستخدمه للتوقيع الالكتروني، ومن مسؤولية صاحبه المحافظة على سريته.

المفتاح العام.

مفتاح ليس سري يستخدم لتشفير الرسائل المرسلة لصاحب هذا المفتاح، وكذلك للتحقق من توقيعه.

هيئة التوثيق (Certification Authority):

هي الجهة التي تقوم بإصدار الشهادة الرقمية والتوقيع عليها، قبل أن تقوم الهيئة بالتوقيع على الشهادة تتأكد من هوية الشخص (صاحب الشهادة) وتتم عملية التأكد من الهوية على حسب استخدامات الشهادة الرقمية فإذا كانت ستستخدم لحماية البريد الإلكتروني فيتم التأكد من هويته بعنوان البريد الإلكتروني فقط أما

إذا كانت لاستخدامات حساسة مثل: إرسال مبالغ كبيرة من المال عن طريق الانترنت فهذه تتطلب حضور الشخص (صاحب الشهادة) إلى هيئة التوثيق للتأكد من هويته وتوقيع الشهادة. وكذلك من خلال هيئة التوثيق يستطيع الشخص أن يجدد شهادته المنتهية، ومن الهيئات comodo و verysign و thwat وهي مواقع موجودة على الانترنت .[10]

هيئة التسجيل (Registration Authority):

هي هيئات تساعد هيئة التوثيق وتخفف الضغط عنها في عمل بعض الوظائف مثل التحقق من الهوية وإصدار التوقيع الإلكتروني.

مخزن الشهادات الرقمية (Certificate Repository):

هو دليل عام متاح للكل تخزن فيه الشهادات الملغاة والفعالة بحيث يستفيد الأشخاص من هذا الدليل للبحث عن المفتاح العام للشخص المراد التعامل معه سواء لتشفير الرسائل المرسلة له بمفتاحه العام لضمان السرية أو لفك التوقيع للتأكد من هوية المرسل.

أهم المعلومات الموجودة في الشهادة الرقمية:

- الرقم التسلسلي: وهو الذي يميز الشهادة عن غيرها من الشهادات.
- خوارزمية التوقيع: الخوارزمية المستخدمة لإنشاء التوقيع الالكتروني.
- صالحة – من: تاريخ بداية صلاحية الشهادة.
- صالحة – إلى: تاريخ نهاية صلاحية الشهادة.
- المفتاح العام: المفتاح العام المستخدم لتشفير الرسائل المرسلة إلى صاحب الشهادة.
- مصدر الشهادة: الجهة التي أصدرت الشهادة.
- أسم مالك الشهادة: سواء كان شخص أو منظمة أو موقع الكتروني

2.2.6.2 أنواع الشهادات الرقمية:

- شهادات هيئة التوثيق:

هذا النوع من الشهادات يصدر من هيئة التوثيق مباشرة وعادة ما يكون لحماية البريد الإلكتروني.

- شهادات الخادم:

هذا النوع من الشهادات يصدر من خادم الشبكة (web server) أو خادم البريد (mail server)

للتأكد من أمان إرسال واستقبال البيانات.

- شهادات ناشر البرامج:

تستخدم للتأكد من أن البرامج الخاصة بناشر معين برامج آمنه.

معيار الشهادة الرقمية (X.509):

هو معيار عالمي أصدره اتحاد الاتصالات الدولي (ITU) لتوحيد شكل وبنية (format) الشهادة الرقمية. أكثر الشهادات الرقمية حاليا تتبع هذا المعيار .

الفرق بين التوقيع الرقمي والشهادة الرقمية:

في التوقيع الرقمي لا يوجد ضمان أن المفتاح العام هو لهذا الشخص بالفعل مثلا يستطيع شخص أن ينشئ له مفتاحين عام وخاص ثم ينشر مفتاحه العام على أساس أنه شخص آخر فلو أراد شخص أن يرسل رسالة سريه لأحد سوف يشفرها باستخدام المفتاح العام الذي نشره الشخص الآخر وبالتالي سوف يستطيع الشخص الآخر فك تشفير الرسالة والإطلاع عليها، أي أنه في التوقيع الرقمي لا يوجد ربط بين الشخص بالفعل ومفتاحه العام لذلك ظهرت الشهادة الرقمية والتي تربط بين الشخص ومفتاحه العام حيث تحتوي الشهادة على صاحب الشهادة ومفتاحه العام وموقعه من طرف موثوق فيه يثبت ذلك .

الشهادة الرقمية للتحقق من الهوية Authentication:

لنفرض أن أحد يريد أن يرسل رسالة لآخر لكي يثبت بأن المرسل هو بالفعل، فانه سوف يوقع المختصر الحسابي (hash) بالمفتاح الخاص فيه ويرسل الرسالة الأصلية والمختصر الحسابي المشفر في الطرف الآخر يقوم بفك تشفير المختصر الحسابي باستخدام المفتاح العام للمرسل الموجود في شهادته الرقمية والمتاحة كما ذكر مسبقا على دليل عام (مخزن الشهادات الرقمية) ثم يقوم بإجراء نفس المختصر الحسابي الذي أجراه على الرسالة بعد ذلك يقارن المختصرين الحسابيين إذا تطابقا فهذا يعني انه بالفعل المرسل، وبهذا ضمنت الشهادة الرقمية التحقق من الهوية، وتسمى العملية السابقة بالتوقيع الإلكتروني.

الشهادة الرقمية لضمان السرية: (Confidentiality)

لنفرض أن أحد يريد أن يرسل رسالة سريه فلكي يضمن سريتها سوف يقوم بتشفير الرسالة بالمفتاح العام للطرف الأخر ولن يفك التشفير إلا بالمفتاح الخاص له (حيث أن المفتاح العام والخاص مربوطان ببعضها أي انه إذا شفرت رسالة بالمفتاح العام لشخص فانه لا يفك تشفير هذه الرسالة إلا بالمفتاح الخاص لنفس الشخص) وبهذا ضمنت السرية.

إدارة الشهادات الرقمية:

يستطيع الشخص أن يختار هيئة التوثيق (CA) التي يريد إصدار شهادته منها وبعد إصدار الشهادة يمكنه تنزيل و تخزين الشهادة والمفتاح العام (public key)على كمبيوتره. بالنسبة لهيئات التوثيق يوجد بعضها تأتي مع متصفح الانترنت في وقت تنزيله ويكون موثوق فيها

3.2.6.2. سياسة الشهادة الرقمية(Certificate Policy):

هي مجموعة من القواعد والسياسات الإدارية والتي تطبق عند إدارة الشهادة الرقمية في جميع مراحل حياتها.

دورة حياة الشهادات الرقمية:

هناك بعض الأحداث التي تؤثر على فعالية الشهادة الرقمية مثل إضافة جهاز (hardware) جديد على الكمبيوتر أو تحديث برنامج وغيره لذلك أصبح للشهادة الرقمية حالات تمر فيها منذ إصدارها.

- **الإصدار:**

وهي أول مرحلة وتشمل التأكد من هوية الشخص قبل الإصدار، ويعتمد التأكد على نوع الشهادة المصدرة ففي الشهادات الرقمية التي تصدر للبريد الالكتروني يتم التأكد من هوية الشخص بطلب إرسال رسالة من بريده الالكتروني فقط أما الشهادات الرقمية المستخدمة للعمليات المالية فتتطلب إجراءات أخرى للتأكد من

الهوية، بعد التأكد من الهوية يتم إرسال الطلب لهيئة التوثيق وتوافق على إصدار الشهادة.

- **الإلغاء:**

يستطيع الشخص أن يلغي شهادته قبل تاريخ انتهائها عندما يفقد المفتاح الخاص بالشهادة أو ينتشر لأنه بعد انتشار المفتاح الخاص تبطل فعالية الشهادة وهي الثقة بالطرف الآخر،(Authentication) ويتم إضافة الشهادة الملغاة إلى قائمة الشهادات الملغاة.

- **الانتهاء:**

لكل شهادة تاريخ انتهاء بعد هذا التاريخ تصبح الشهادة غير صالحه للاستخدام ولابد من إصدار شهادة جديدة ويمكن أن تكون الشهادة الجديدة لها نفس المفتاح العام والخاص للشهادة المنتهية.

- **التعطيل المؤقت:**

يمكن للشخص أن يوقف أو يعطل استخدام الشهادة لفترة زمنية لا يحتاج فيها لاستخدام الشهادة حتى لا تستغل من قبل أشخاص آخرين[10].

وتقوم العديد من الجهات (Certificate Authority) بتوليد ومنح الشهادات الرقمية مثل www.verisign.com، ومنها ما هو مجاني وغير مجاني، وتقوم جهات أخرى بدور Registration Authority وهو تسجيل وتوثيق الشهادات والتأكد من هوية أصحابها.

ليس من الصعب كما قد يبدو للوهلة الأولى الحصول على تلك الشهادات، فيمكن توليد تلك الشهادات من مخدم (Microsoft Windows Server) ولكن مصداقية وموثوقية الشهادة مكافئة لمصداقية وموثوقية الجهة المانحة ، مثلاً شهادة ممنوحة من شركة مايكروسوفت تحمل بالتأكيد مصداقية عالمية بينما لو قمت بتوليد شهادة من مخدم محلي على النطاق، (MyCompanDdomain.local) فإن مصداقيتها محدودة بمن يثق في هذا النطاق.

3.6.2. التوقيع الالكترونيelectronic signature

في الآونة الأخيرة دعت الحاجة لاستخدام التقنية في شتى المجالات بسبب انتشار استخدام الانترنت، فلا يكاد يخلو بيت أو شركة أو بنك أو جهة حكومية من حاسب آلي، فهو يوفر الوقت والجهد فعن طريق الانترنت يتم تبادل الوثائق والملفات و من خلاله أخذت المستندات الورقية في التراجع شيئاً فشيئاً، لذلك دعت الحاجة لتشفير البيانات بشتى الطرق، لتوفير الأمان للملفات وللمستخدمين من العبث والتزوير وللتأكد أيضا من صحة هذه البيانات فظهر ما يعرف بالتوقيع الالكتروني الذي يضمن للمستقبل والمرسل صحة ومصداقية وخصوصية هذه البيانات.

1.3.6.2.ما هو التوقيع الالكتروني electronic signature

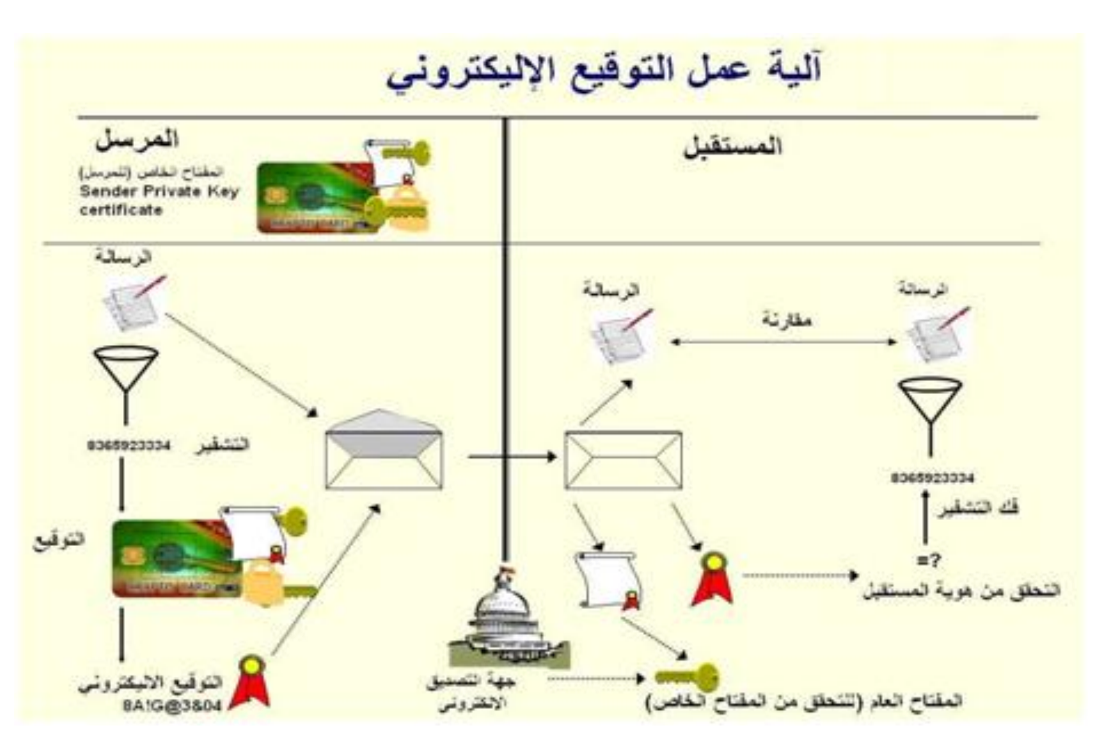
هو عبارة عن عملية تشفير مكون من بعض الحروف والرموز والأرقام الإلكترونية، تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا.

تعمل على توثيق الملفات بشتى أنواعها والتي تتم عبر الإنترنت، فيتم من خلالها ربط هوية الموقع بالوثيقة، وبحيث يمكن لمستلم الوثيقة التحقق من صحة التوقيع، وأيضا من السهل لكل شخص الحصول على هذا التوقيع من الجهات المختصة لإصدار الشهادات، فيستخدم هذا التوقيع لإغراض عدة منها أغراض الشخصية و سياسيه أو تجاريه، وغيرها من المجالات الأخرى، فقد اهتمت معظمدول العالم بالتوقيع الالكتروني وأصدرت نظام التعاملات الالكترونية مما دعم استخدام التوقيع الالكتروني في التعاملات الالكترونية، أيضا أصدرت نظام أخر يخص بالجرائم المعلوماتية للحد من التزوير والغش وانتحال الشخصية [14].

2.3.6.2.كيفية عمل التوقيع الالكتروني :

لعمل التوقيع الالكتروني لابد من التقدم إلى إحدى الجهات المختصة بإصدار الشهادات حتى يتم إصدار الشهادة للمستخدم، ويكون معها مفتاحين احدهما عام والأخر خاص، فعندما يرسل هذا المستخدم المالك لشهادة رسالة سوف يتم تشفيرها بالمفتاح الخاص به أو المفتاح العام التابع للمستقبل، بحيث تتحول هذه الرسالة إلى رموز لا يمكن فهمها ويتم إرفاق معها توقيع المرسل.

عند إذن يقوم المستقبل بإرسال نسخه من التوقيع الالكتروني إلى الجهة المختصة بإصدار الشهادة، لتأكد من صحة التوقيع ومن ثم تقوم أجهزة الكمبيوتر التابعة للجهة المختصة بالتحقق من صحة التوقيع وتعاد النتيجة للمستقبل مرة أخرى، ليتأكد من صحة وسلامة الرسالة، فيقوم المستقبل بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على أساس رقمه العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، ومن ثم يجيب على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية، ويستخدم أيضا مع التوقيع الالكتروني عملية الهاش التي توفر اقل تكلفه من تشفير الرسالة بحيث تقوم بإنشاء قيمة رقمية معينة تكون اصغر من الرسالة بحيث تضمن الرسالة من أي تغيير يتم عليها بحيث عندما يستقبل المستخدم الرسالة والهاش يقوم بعملية الهاش مرة أخرى على الرسالة ومن ثم يقارن الهاش الذي استقبله بالهاش بالذي عمله إذا كانت متساوية فيدل على سلامة البيانات من التحريف والتزوير وإذا اختلفت دل على تزويرها [14] كما في الشكل (4.2).



شكل (4.2) : يوضح آلية عمل التوقيع الالكتروني .

3.3.6.2.أنواع التوقيعات الالكترونية:

يوجد نوعين شائعين احدهما التوقيع المشفر الذي تحدثنا عنه، التي يقوم المرسل بإرسال الوثيقة مشفره معها توقيعه المكون من معلوماته. أما النوع الآخر ما يعرف بالتوقيع البيومتري، الذي يتم تحديده عن طريق تحريك يد الموقع أثناء التوقيع، بحيث يتم توصيل قلم إلكتروني بجهاز الكمبيوتر، ويقوم الموقع بالتوقيع باستخدام هذا القلم الذي يسجل حركات يد المستخدم أثناء التوقيع ، حيث إن لكل شخص سلوكا معينا أثناء التوقيع [14] كما في الشكل.



شكل (5.2) : التوقيع البيومتري .

4.3.6.2. أهمية التوقيع الالكتروني:

فالغرض منه لتصديق أن الرسالة لم يتم تغييرها، وتوفر الضمان والتأكد بأنه لم يتم أجراء أي تعديل على الرسالة لأنه من الصعب تزويره والعبث به، فهو أيضا يوفر 4 خواص وهي:

1- الخصوصية: بحيث يمنع أي مستخدم غير شرعي من تعديل أي إجراء على البيانات.

2- التحقق من هوية المرسل: ومصادر البيات عن طريق جهة الشهادات التصديق الالكترونية المرخص لها دوليا.

3- التحقق من هوية المستخدم: لوحدة البيانات من تعويضه من بيانات أخرى باستخدام تقنيه تشفير البيانات ومقارنته بصمة الرسالة المرسلة ببصمة الرسالة المستقبلة.

4- خاصية عدم الإنكار: عدم قدرة المرسل من الإنكار لوجود الطرف الثالث "جهة تصديق معينه" وعدم قدرة المستقبل أيضا بالإنكار من استقبال الرسالة بحيث تكون هذه الجهة وسيطة بين المرسل والمستقبل بحيث كلما أراد المرسل أن يرسل رسالة لابد أن تمر على هذه الجهة المختصة، وكذالك كلما استقبل المستقبل الرسالة [14].

الفصـــــــــل الثالث

أمــن طبقة التطبيقات

الفصل الثالث: الاختراقات وطرق تأمين طبقة التطبيقات

1.3.امن طبقة التطبيقات

مقدمة

كما ذكرنا سابقا (في الفصل الأول) فان طبقة التطبيقات Application layer هي الطبقة العليا في نموذج وصل الأنظمة المفتوحة OSI. وهذه الطبقة توفر خدمات الشبكة للمستفيد النهائي وهي تستفيد من الطبقات التي تحتها ولكنها معزولة تماما عن تفاصيل المعدات والأجهزة. وتتعامل هذه الطبقة مع البيانات المرسلة إلى والواردة من الطبقة السادسة بالنموذج، وهي طبقة التمثيل Presentation layer ، حيث تحدد الطريقة التي تتفاعل بها البرامج التطبيقية application programs مع الشبكة، فهي تقدم خدمات التطبيقات مثل خدمة انتقال الملفات، والبريد الإلكتروني، وإدارة قواعد البيانات، وبرامج محاكاة الطرفيات terminal emulation، وأي خدمات تقدمها برامج الشبكة، وخدمات الشبكة في هذه الطبقة تكون عادة بروتوكولات تتعامل مع بيانات المستفيد والتطبيقات HTTP، Telnet،SMTP، FTP هي تطبيقات توجد في هذه الطبقة، فمثلا، في حالة التطبيق المتعلق بمتصفح الويبWeb browser، فإن بروتوكول طبقة التطبيقات HTTP، يغلف البيانات المطلوبة لإرسال واستقبال محتويات صفحة الويب Web [12][13] page.

2.3.البروتوكولات التي تعمل في طبقة التطبيقات:

1.2.3. Hyper Text Transfer Protocol (HTTP)

وهو الطريقة الرئيسة والأكثر انتشاراً لنقل البيانات في الويب(www) الهدف الأساسي من بنائه كان إيجاد طريقة لنشر واستقبال صفحات HTML.

HTTP هو نظام نقل مواد الإنترنت عبر الشبكة العنكبوتية الويب، وهو من الطبقة الخامسة لنظام TCP/IPوهي طبقة التطبيقات ويستخدم من قبل متصفحات الإنترنت والتي تسمى عميل المستخدم–user agent ويستخدم المدخل رقم 80 على المخدم غالبا بالتعاون مع الطبقة الرابعة وبالتحديد مع ميثاق

(بروتوكولTCPللحصول على الصفحات المطلوبة وبعد ذلك تبدأ مهمة بروتوكول TCP لتولى المهمة من هنا والبدء في عمله.

HTTP الآمن :

حاليا هناك طريقتان لإنشاء اتصال HTTP آمن : مخطط HTTPS URI ورأس ترقية HTTP 1.1 ، الذي قدم بواسطة RFC 2817 دعم المتصفح لرأس الترقية، يكاد يكون غير موجود، وبالتالي مخطط HTTPS URI لا يزال الأسلوب المهيمن لإنشاء اتصال HTTP آمن HTTP .الآمن يبدأ بHTTPS :// بدلاً من HTTP ://



مخطط HTTPS URI

HTTPS هو مخطط URI مطابق في بنائه لمخطط HTTP الذي يستخدم في اتصالات HTTP المعتادة، لكنه يشير للمتصفح باستخدام طبقة تشفير إضافية من SSL/TLS لحماية حركة المرور SSL . ملائمة بصفة خاصة HTTP لأن بإمكانها أن توفر بعض الحماية حتى إذا كان جانب واحد فقط من الاتصال موثقاً، هذا هو الحال مع معاملات HTTP عبر الإنترنت، حيث يكون الخادم فقط موثقاً عن طريق فحص العميل لشهادة الخادم.

رأس ترقية HTTP 1.1

HTTP 1.1 قدم الدعم لرأس الترقية. في عملية التبادل، يبدأ العميل بتقديم طلب واضح النص، الذي يتم في وقت لاحق رفع مستواه TLS قد يطلب العميل أو الخادم رفع مستوى الاتصال. تقديم طلب واضح النص من قبل العميل يليه طلب الخادم رفع مستوى الاتصال هو الاستخدام الأكثر شيوعا، ويبدو كما يلي:

العميل:

```
GET /encrypted-area HTTP/1.1
Host: www.example.com
```

الخادم:

```
HTTP/1.1 426 Upgrade Required
Upgrade: TLS/1.0, HTTP/1.1
Connection: Upgrade
```

قام الخادم بإرجاع رمز الحالة 426 لأن مستوى الرموز 400 يشير إلى فشل العميل، ويعمل على تنبيه العملاء بأن الفشل كان ذا صلة بالعميل.

فوائد استخدام هذا الأسلوب لإنشاء اتصال آمن:

1. أنه يزيل الفوضى وإشكالية إعادة التوجيه وإعادة كتابة العنوان من جهة الخادم.
2. أنه يسمح بالاستضافة العملية للمواقع المضمونة على الرغم من أن HTTPS يسمح بهذا وذلك باستخدام دلالة اسم الخادم.
3. أنه يقلل من إرباك المستخدم من خلال توفير وسيلة وحيدة للوصول إلى مورد معين.

نقطة الضعف في هذه الطريقة هي أن الحاجة إلى HTTP آمن لا يمكن تحديدها في URI في الممارسة العملية، الخادم (الغير موثوق به) سيكون المسؤول عن تمكين HTTP الآمن، وليس العميل الموثوق[14].

حيث HTTP:يؤمن تصفح صفحات الويب عن طريق تأمين تناقل المعطيات بين مخدم الويب web ومتصفح الويب web browser.

2.2.3.(FTP) File Transfer Protocol

يعتبر بروتوكول نقل الملفات FTP أحد المواثيق التي تنضم لحزمه مواثيق TCP أو Transmission Control Protocolsفي النقل وهي تتميز بالأمان في نقل البيانات والتأكد من عدم فقدان البيانات خلال النقل.

يتميز بروتوكولFTP باستخدام منفذ port20 ، المنفذ الأول رقمه 21 وهو مسئول عن نقل الأوامر بينما يستخدم المنفذ رقم 20 من اجل نقل البيانات.

أهداف FTP

إنّ أهداف FTP، كما هو ملخّص من قبل RFC الخاص به، هي:

1. ترويج اشتراك الملفات (برامج الحاسوب أو البيانات).
2. تشجيع الاستعمال غير المباشر أو الضمني للحواسيب البعيدة.
3. حماية المستخدم من الاختلافات في أنظمة تخزين الملف بين المضيّفين المختلفين.
4. تحويل البيانات بشكل موثوق وكفؤ[16].

حيث يمكن أن نقول أن وظيفته في طبقة التطبيقات تأمين تناقل الملفات عبر الشبكة .

3.2.3. Simple Mail Transfer Protocol (SMTP)

البروتوكول SMTP :

يعد بروتوكول نقل الرسائل البسيط Simple Mail Transfer Protocol أو SMTP اختصاراً البروتوكول المعياري لنقل الرسالة من الزبون إلى المخدم بشكل موثوق وفعال .

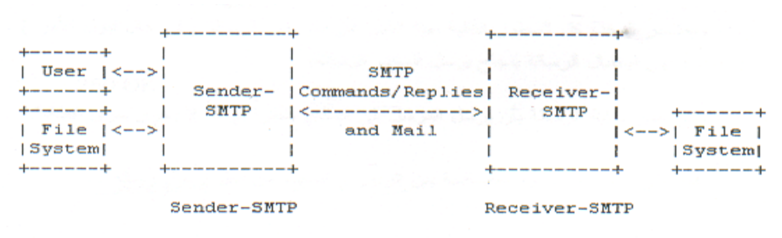
تم توصيف هذا البروتوكول لأول مرة عام 1980 وتم اقتراح عدة تعديلات عليه حتى تم اعتماده بشكل رسمي كبروتوكول قياسي لنقل الرسائل على الشبكة , وتم توصيفه عام 1981 تحت العنوان RFC 821

يتصل برنامج قارئ البريد بمخدم الرسائل الصادرة SMTP Server مستخدماً المنفذ 25 .

يتم إجراء تخاطب بين الطرفين يخبر فيه الزبون المخدم بالمعلومات اللازمة للإرسال مثل عنوان المرسل والمستقبل [9].

تبدأ عملية الإرسال بأن يطلب المرسل SMTP Sender فتح رابطة ثنائية مع المخدم SMTP Receiver ومن ثم يولد الزبون عدة أوامر ويرسلها إلى المخدم من أجل تعريف نفسه ويجيب المخدم

على كل أمر برسالة أخرى يرسلها الزبون ، وعندما تتم الموافقة على فتح الرابطة بين الطرفين يتم تبادل الأوامر والمعطيات بينهما، ومن ثم يتم إنهاء الاتصال بينهما، كما في الشكل التالي



Model for SMTP Use

نموذج (SMTP(SMTP Model :

عندما يعلن المستخدم عن رغبته في إرسال رسالة، فإن قارئ البريد أو (SMTP Sender مثلاً برنامج Out look يقوم بالاتصال بمخدم الرسائل الصادرة أو SMTP Receiver وهذا المخدم هو عبارة عن حاسب يحوي على البرمجيات المناسبة لخدمة البريد الإلكتروني، مثلاً Exchange Server، وبهذا

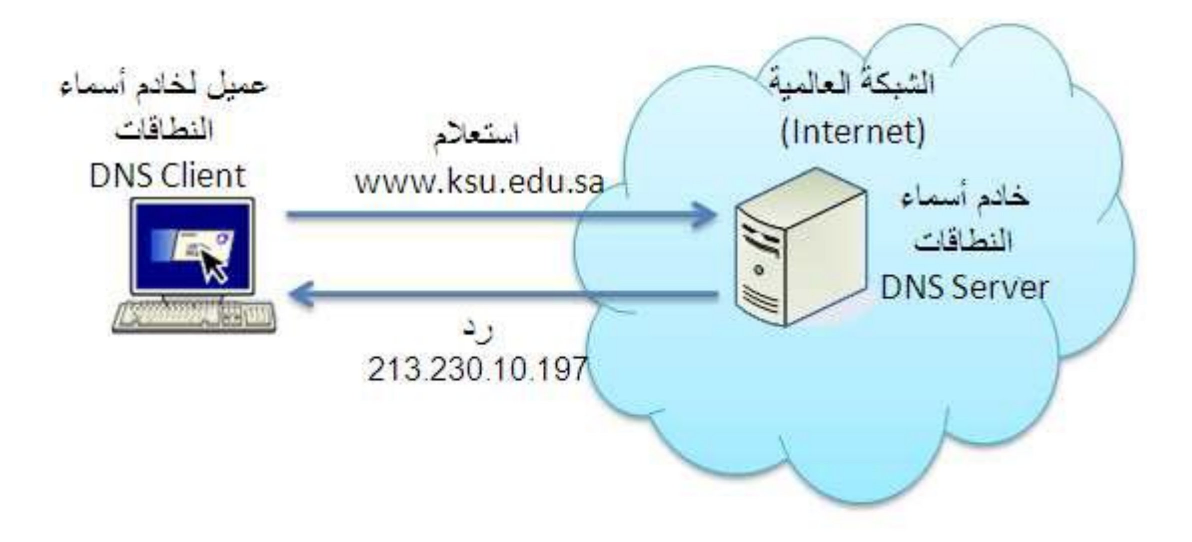
يؤمن تراسل البريد الإلكتروني عبر الشبكة .

Telnet،DNS،SNMP

ومن الملاحظ أن تطبيقات المستخدم النهائية لا تعمل ضمن طبقة التطبيقات فمتصفح الويب مثلا ليس من طبقة التطبيقات ولكنه يستخدم البروتوكول HTTP الذي ينتمي إلى طبقة التطبيقات من أجل التخاطب مع مخدم الويب[13].

DNS.4.2.3 نظام أسماء النطاقات اختصار لجملة Domain Name System هو نظام يخزن معلومات تتعلق بأسماء نطاقات في قاعدة بيانات موزعة على الإنترنت.يقوم خادماسم النطاق بربط العديد من المعلومات بأسماء النطاقات، ولكن وعلى وجه الخصوص يخزن عنوان IP المرتبط بذلك النطاق.

بمعنى آخر هو نظام يقوم بترجمة أسماء النطاقات من كلمات إلى أرقام تعرف باسم(IP Address)



شكل(1.3) يوضح نظام أسماء النطاقات

إذا أردنا الاتصال بأي موقع علينا معرفة IP الخاص بهذا الموقع، فهناك ما يسمىDomain Names، أو أسماء النطاقات، حيث أنه يكفي للاتصال بموقع ما أن نعرف اسم النطاق الخاص بهذا الموقع، عندما نكتب هذا العنوان في المتصفح ، فإن الخطوة الأولى التي يقوم بها المتصفح هي الاستعلام عن IP الخاص بهذا الموقع، ويتم هذا عبر DNS، أو نظام أسماء النطاقات، وهذا عن طريق خادم يترجم أسماء النطاقات، إلى عناوين IP، اللازمة للحاسوب كي يقوم بالاتصال مع الموقع.

يعتبر نظام أسماء النطاقات مفيداً لعدة أسباب، أكثرها وضوحا، أنه يجعل من الممكن استبدال عناوين IP الصعبة التذكر مثل 207.142.131.206 بأسماء نطاقات سهلة التذكر، وهذا يسهل على البشر التعامل مع عناوين الشبكة وعناوين البريد الإلكتروني، كما أن النظام يسمح بإنشاء أسماء معترف بها ويمكن الوصول إليها دون الاتصال مع التسجيل المركزي في كل مرّة .

Telnet.5.2.3 يعتبر بروتوكول من بروتوكولات TCP/IP للاتصال بأجهزة الكمبيوتر البعيدة، كما أنه تطبيق من تطبيقات TCP/IP يتم استخدامه في تشغيل برامج telnet لكي يتيح إمكانية التحكم عن بعد ويسمح للمستخدم الدخول من حاسوبه الشخصي إلى حاسب آخر وأن يقوم بالعمل كما لو كان متصل مباشرة مع الجهاز البعيد واستخدام مصادره وهذه المصادر ممكن أن تكونonline database، chat services .[27]

أهم ميزات خدمات Telnet

1. يمكنك استخدام Telnet كمتصفح ويب لأي موقع، ولكنه سيعرض لك مصدر الصفحة حصرا أي Source للصفحة، وذلك لأن خدمة Telnet كانت تُستخدم عندما كانت مواقع الإنترنت مجرد نصوص.

2. ويمكن استخدام Telnet أيضا كـ FTP Client وذلك باستخدام أوامر يتم إدخالها من خلال telnet

3.ويمكنك من خلال Telnet أيضا تصفح الايميل POP Mail وقراءة رسائلك الواردة وإرسال ما تريد من رسائل،إذا كان الايميل من نوع POP Mail وهو اختصار.Post Office Protocol

6.2.3.بروتوكولSNMP(Simple Network Management Protocol)

هذا البروتوكول هو عبارة عن الطريقة التي يتم من خلالها إدارة اغلب شبكات TCP/IP.

ويتوقف البروتوكولSNMP على ترتيب البرنامج المسئول عن تجميع المعلومات والبرنامج المسئول عن الإدارة، إذ يعمل برنامج تجميع المعلومات على تجميع معلومات حول الجهاز المضيف، في حين يعمل البرنامج المسئول عن الإدارة على الحصول على معلومات الحالة فيما يتعلق بأجهزة الكمبيوتر المضيفة، وذلك من خلال تعداد برامج تجميع المعلومات وقبول المعلومات الصادرة عنها[2].

3.3.وسائل تحقيق الأمن في طبقة التطبيقات

امن طبقة التطبيقات(Security of Application Layer)

كل طبقة من طبقات OSI لديها قناعاتها وتحديات أمنية فريدة من نوعها طبقة التطبيقات هي حلقة ضعيفة جدا من الناحية الأمنية لأن طبقة التطبيقات تدعم العديد من البروتوكولات التي توفر العديد من نقاط الضعف ونقاط الوصول للمهاجمين، كل هذا التنوع يجعل من طبقة التطبيقات من الصعب جدا للدفاع عنها، وبالإضافة إلى ذلك، طبقة التطبيقات هي جذابة للغاية لمهاجم محتمل لأن المعلومات التي يسعون يقيم في نهاية المطاف ضمن التطبيقات نفسها وأنها هدف مباشر بالنسبة لهم ليكون لها تأثير وتحقيق أهدافهم .[18]

1.3.3.الفئات الرئيسية للمخاطر على مستوى التطبيقات هي كما يلي:

الأمن على شبكة الإنترنت: التوازن بين الأمن وسهولة الوصول إليها، سرقة المعلومات السرية، وتعديل أنظمة وشن هجمات مختلفة من ناحية أخرى، فيروس /دودة: إلى المستخدم النهائي، المحتوى النشط، مثل عناصر تحكم ActiveX وتطبيقات جافا، ويدخل في ذلك إمكانية تصفح الإنترنت وسوف تنقل فيروسات أو البرامج الضارة الأخرى في النظام المستخدم لمدير الشبكة، ومتصفحات الويب مع المحتوى النشط توفر طريقا للبرمجيات الخبيثة للالتفاف على نظام جدار الحماية والدخول على الشبكة المحلية.

خصوصية المعلومات: كل من المستخدمين النهائيين ومديري ويب مدعوون للقلق على سرية البيانات المنقولة عبر شبكة الانترنت.

أمن البريد الإلكتروني: إذا كان الاتصال بخادم بريد الويب الخاص بك هو "غير آمن" (أي عنوان هو //:http و//:https)، ثم كل المعلومات بما في ذلك اسم المستخدم وكلمة السر غير مشفرة لأنها تمر بين واجهة الخادم وجهاز الكمبيوتر الخاص بك SMTP: SMTP لا تشفر الرسائل بالإضافة إلى ذلك، اسم المستخدم وكلمة السر "الدخول" إلى خادم SMTP هي أيضا في نص عادي .قد تكون هذه المعلومات متاحة لجميع المستفيدين، تشكل مصدر قلق الخصوصية POP و IMAP هذه البروتوكولات تتطلب منك

إرسال اسم المستخدم وكلمة السر للدخول، والتي هي غير مشفرة .هكذا، يمكن قراءة الرسائل وأوراق الاعتماد من قبل أي متنصت للاستماع إلى تدفق المعلومات بين الكمبيوتر الشخصي وجهاز كمبيوتر مزود خدمة البريد الإلكتروني، حيث يعتبر فيروس / دودة: البريد الإلكتروني هي ناقل نشطة للغاية من الفيروسات والديدان[18].

هجوم كلمة السر: يشار إلى هجوم كلمة السر من خلال سلسلة من عمليات تسجيل الدخول الفاشلة في غضون فترة قصيرة من الزمن، كلمة السر أدوات الحفظ معظم التدقيق يتضمن جداول كلمة السر قبل محسوب يحتوي على تريليونات من التجزئة كلمة السر التي تم حسابها في وقت سابق لتدقيق كلمة المرور وعملية الاسترداد .

هجومDNS: ويسمى أيضا DNS الغش أو DNS مخبأ التسمم، انه من الهجمات التي تهدف إلى إعادة توجيه المستخدمين إلى خوادم الويب المحتمل أن تكون ضارة من خلال تغيير السجلات المستخدمة لتحويل أسماء النطاقات إلى عناوين رقمية، والذي يستخدم في طريقة أخرى للمحتالين على الإنترنت لتثبيت الدعاية العدوانية البرامج، أو ادواري، وعلى أجهزة كمبيوتر الضحايا وتوجيه الناس بالنقرة على المواقع على شبكة الإنترنت، نظام اسم المجال هو بروتوكول ضعيف أصلا في هذا النمط من الهجوم بسبب ضعف معاملات المعرفات 16 بت .

لحظة أمن الرسالة: أكثر المخاطر الأمنية هي: الفيروسات والديدان خلال التراسل الفوري، وانتحال الهوية سرقة / التوثيق، ونفق جدار حماية أمن البيانات و التسريبات، والرسائل الفورية غير المرغوبة.[18]

هجوم:SNMP معظم أجهزة دعم إدارة الشبكة البسيط (SNMP) لشبكة رصد الغرض .حيث يتمكن المهاجمين من الوصول إلى MIBs من وكلاء SNMP الذي يمكن أن ينتج عنه تعيين الشبكة، يمكن رصدها والاتجار بها وتوجيهها، أفضل وسيلة للدفاع ضد هذا الهجوم هو الترقية إلىSNMP3 ، الذي يشفر كلمات المرور والرسائل [18].

مخاطر نظم التشغيل: جميع أنظمة التشغيل ليست آمنة، وخاصة نظام التشغيل ويندوز وأنظمة يونيكس . التطبيقات الأخرىFTP و Telnet بعض الإصدارات القديمة من تطبيقات الشبكة مثل بروتوكول نقل الملفات سلبية ويرجح مع الثغرات الأمنية .ينبغي الحصول على أحدث الإصدارات من المنتجات تنفذ بقع الأمنية الأخيرة مع معظم مشاكل أمن الشبكة، وليس هناك حل سحري لعلاج هذه المشاكل، ومع ذلك، هناك العديد من التقنيات والحلول المتاحة للتخفيف من حدة المشاكل الأمنية أعلاه، وعلى رصد شبكة للحد من الأضرار في حال هجوم يحدث، للتخفيف من حدة المشاكل الأمنية لطبقة التطبيقات، وقد وضعت العديد من التقنيات في مستويات مختلفة من الاتصالات[18].

2.3.3 التقنيات الرئيسية هي كما يلي:

الآمنMultipurpose / ملحقات بريد إنترنت (S / MIME) هي مواصفات لتأمين البريد الالكتروني S / MIME، الذي يقوم على أساس معيار MIME الشعبية، ويصف مشروع بروتوكول لإضافة خدمات تشفير أمني من خلال تغليف MIME من الكائنات التي تم توقيعها رقميا ومشفرة،هذه الخدمات الأمنية والتوثيق، و non repudiation، سلامة الرسالة، ورسالة سرية .

الخصوصية (PGP) هو يستخدم عمدا خوارزميات التشفير القائمةRSA، IDEA، MD5 بدلا من اختراع جديد PGP يدعم سرية، والتوقيعات الرقمية، وإدارة المفتاح، وضغط البيانات[18].

آمن HTTP (S-HTTP) هو مجموعة شاملة منHTTP ، والذي يسمح لتكون مغلفة حركة المرور على الشبكة بطرق مختلفة S-HTTP .يوفر تشكيلة واسعة من آليات، والسرية المصادقة والنزاهة.وكان الفصل بين السياسة العامة من آلية هدفا واضحا، لا يرتبط نظام S-HTTP إلى أي نظام تشفير خاص، والبنية التحتية الأساسية، أو شكل التشفير .

البنية التحتية للمفتاح العامPKI :(PKI) يوفر حلا متكاملا مع الشهادات الرقمية، وتشفير المفتاح العام، والسلطات الشهادة التي تمكن الشركات من أجل حماية أمن الاتصالات والمعاملات التجارية على شبكة الإنترنت، نموذجي شبكة PKI يشمل إصدار شهادات رقمية للمستخدمين الأفراد والخوادم، للمستخدم النهائي

البرمجيات الالتحاق؛ التكامل مع الدلائل شهادة الشركات، وأدوات لإدارة وتجديد، وشهادات إلغاء، والخدمات ذات الصلة ودعمها [3].

لمكافحة الفيروسات هناك أنظمة: العديد من المنتجات في العميل أو مستوى الملقم تعمل لاعتقال وقتل الفيروسات من مصادر مختلفة بما في ذلك حركة HTTP ويب، والبريد الإلكتروني والخدمات.

وهناك العديد من تقنيات الطبقة السفلى التي تدعم أمن طبقة التطبيقات وفيما يلي بعض الأمثلة: طبقة مآخذ التوصيل الآمنة (SSL) وأمن طبقة النقل (TLS) لبروتوكولات التشفير التي توفر اتصالات آمنة على الإنترنت TLS هو successor من SSL, TSL / SSL يعمل على طبقات تحت بروتوكولات التطبيق مثلHTTP ، SMTP و NNTP وفوق بروتوكول النقل TCP في حين TSL / SSL يمكن أن تضيف إلى أي أمن بروتوكول يستخدم برنامج التعاون الفني، هو الأكثر شيوعا مع HTTP لتشكيل HTTPSوالذي يعمل على تأمين صفحات الشبكة العالمية للبريد[18].

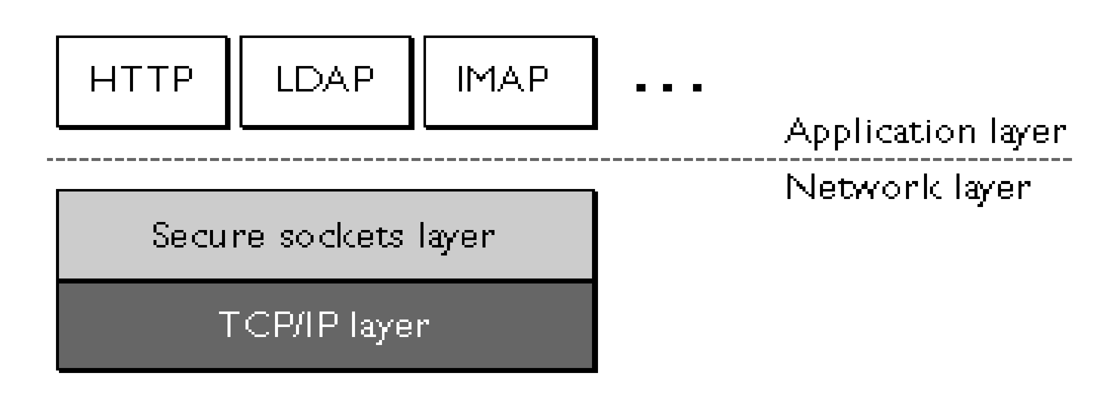
أمن بروتوكول الإنترنت: أمن بروتوكول الإنترنت تقدم خدمات الأمن في طبقة الملكية الفكرية من خلال تمكين نظام لتحديد البروتوكولات الأمنية المطلوبة، وتحديد خوارزمية لاستخدامها في خدمة ، ووضعها في أي مكان مفاتيح التشفير اللازمة لتقديم الخدمات المطلوبة .

جدار الحماية: منتجات جدار الحماية مصممة لحظر الزوار المتطفلين وحركة المرور الضارة .[18] وفيما يلي سنقوم بشرح مفصل لأهم التقنيات المستخدمة في أمن طبقة التطبيقات.

3.3.3.بروتوكول طبقة المقبس الآمن (Secure Socket Layer Protocol (SSL

لاقى SSL قبولا واسعا كبروتوكول للتحقق من هوية طرفي الاتصال وتشفير المعلومات المتبادلة بينهما، صمم البرتوكول في الأساس من قبل شركة Netscape وحاليا أصدر مجلس IETF(Internet Engineering task Force) معيارا جديدا هو TLS(Transport Layer Security) والمبني بالاعتماد على بروتوكول SSL، ويتوقع أن تقوم Netscape بدعم هذا البروتوكول في معظم منتجاتها .

يقدم بروتوكول TCP/IP (Transmission Control Protocol/Internet Protocol) خدمة النقل والتوجيه للبيانات على الإنترنت ، وتقوم بروتوكولات التطبيقات باستخدام TCP/IP لأداء مهامها ومن هذه البروتوكولات HTTP ، SMTP ، ... ، ولكن يفتقر بروتوكول TCP/IP إلى الأمن والسرية في نقله للمعلومات مما أظهر الحاجة إلى وجود طبقة وسيطة بين بروتوكول النقل وبروتوكولات التطبيقات .



شكل(2.3) يوضح الطبقات التي يأمنها SSL

إن بروتوكول SSL يعمل فوق بروتوكول TCP/IP وتحت طبقة التطبيقات ، بحيث يستعمل SSL بروتوكول TCP/IP لنقل البيانات بعد تطبيق العمليات اللازمة لضمان الأمان والسرية في النقل .

1.3.3.3 مهام SSL :

1. التحقق من هوية المخدم : يستطيع المستخدم بواسطة هذا البروتوكول التحقق من هوية المخدم الذي يتعامل معه وذلك باستخدام تقنيات معيارية للتشفير بالمفتاح العام، حيث يتم التحقق من الشهادة الرقمية للمخدم فيما إذا كانت صالحة وصادرة من جهة موثوقة بالنسبة للزبون ويتم التحقق أيضا من المفتاح العام المرتبط معها وتعد هذه العملية ذات أهمية كبرى للمستخدم حيث يحتاج ضمانة إلى أن أحدا لن ينتحل شخصية البنك ويقوم بالتقاط رقم بطاقة اعتماده مثلا عندما يرسلها على الشبكة .

2. التحقق من هوية الزبون : يتم في هذه المهمة عمل نفس الخطوات في الوظيفة السابقة ولكن هذه المرة يحتاج المخدم إلى التحقق من شرعية الزبون ويقوم بذلك بنفس التقنيات أيضا.
3. الاتصال المشفر : تهتم الوظيفتان السابقتان بالتحقق لكل طرف من هوية الطرف السابق ولكن قد يحتاج الطرفان إلى عدم اطلاع طرف ثالث على المعلومات المرسلة أيضا ، لذلك يؤمن SSL بناء اتصال مشفر بين الطرفين مما يمنح سرية عالية للاتصال، ولكن بقيت لدينا مشكلة وحيدة وهي العبث بالمعلومات، يقوم SSL بحل هذه المشكلة حيث يقوم بشكل تلقائي من أن المعلومات لم تتغير منذ إرسالها [9].

2.3.3.3 بنية بروتوكول SSL

يتألف بروتوكول SSL من برتوكولين جزئيين :

1. بروتوكول سجل SSL : حيث يعرف البنية المستخدمة لإرسال المعلومات .
2. بروتوكول المصافحة في SSL : يغلف بواسطة البروتوكول الجزئي الأول حيث يقوم بتبادل سلسلة من الرسائل بين SSL المخدم و SSL الزبون وذلك عند بدء تأسيس اتصال SSL، يتم في هذه السلسلة من الرسائل تحقيق الوظائف السابقة :

- ✓ التحقق من هوية المخدم لصالح الزبون .
- ✓ اختيار المشفر أو خوارزمية التشفير التي يستطيع كلا الطرفين دعمها .
- ✓ التحقق من هوية الزبون وذلك في حال طلب المخدم ذلك .
- ✓ استخدام تقنية التشفير بالمفتاح العام لتوليد سرية مشتركة لكليهما .
- ✓ تأسيس اتصال SSL المشفر .

3.3.3.3 خوارزميات التشفير المستخدمة في SSL

- يدعم SSL عددا من خوارزميات التشفير التي يستخدمها في العمليات المختلفة مثل إرسال الشهادة الرقمية وتوليد مفاتيح الجلسة وما إلى ذلك ، قد يدعم كل من الزبون والمخدم مجوعة مختلفة من خوارزميات التشفير وذلك عائد إلى عدة عوامل منها اختلاف نسخ SSL التي يعمل عليها كل منهما أو

اختلاف درجة الحماية المطلوبة من عملية لأخرى أو القوانين التي تمنع استخدام خوارزميات تشفير محددة .

- تمنح خوارزميات تبادل المفتاح مثل KEA و RSA طريقة لـ SSL لتحديد مفتاح التناظر الذي سوف يستخدم خلال جلسة عمل SSL ، الخوارزمية الأكثر استخداما هي RSA key exchange
- يوجد مجموعة من خوارزميات التشفير والمدعومة من قبل SSL 2.0 و SSL 3.0 ، لذلك يستطيع المسؤول عن الأمن في الشبكة أن يقوم بإلغاء تمكين بعض الخوارزميات وذلك حسب القوة المطلوبة للتشفير والتي تعتمد بشكل أساسي على نوع المعلومات المراد نقلها ومدى سريتها والسرعة المطلوبة ، حيث يقوم الطرفان بالتفاوض على استخدام الخوارزمية ذات القوة الأعلى والمطلوبة من أحدهما .

4.3.3.3 المصافحة في SSL

تعد الخوارزميات التي تستخدم المفتاح المتناظر أسرع من خوارزميات المفتاح غير المتناظر و المفتاح العام، ولكن خوارزميات المفتاح العام أفضل من حيث التحقق من الهوية، لذلك تستخدم SSL مزيج من هذه التقنيتين، حيث تقوم في بداية فتح اتصال SSL بتبادل عدد من الرسائل تدعى بالمصافحة، تستخدم في المصافحة تقنية المفتاح العام للتحقق من هوية المخدم من قبل الزبون، وبعد إتمام هذه العملية بنجاح يتعاون الطرفان في إنشاء المفاتيح المتناظرة التي ستستخدم في الجلسة للتشفي وفك التشفير وكشف محاولات العبث بالمعلومات، يتم بعد ذلك وبشكل اختياري التحقق من هوية الزبون .

1.4.3.3.3 خطوات المصافحة :

1. يرسل الزبون إلى المخدم نسخة SSL التي يدعمها وإعدادات المشفرات وبعض البيانات المولدة عشوائيا بالإضافة إلى معلومات أخرى يستخدمها المخدم في الاتصال مع الزبون .
2. يرسل المخدم إلى الزبون نسخة SSL التي يدعمها وإعدادات المشفرات وبعض البيانات المولدة عشوائيا بالإضافة إلى شهادة المخدم الرقمية ، وفي حال كان المخدم يحتاج إلى التحقق من هوية الزبون يرسل أيضا طلب تحقق من هوية الزبون .
3. يقوم الزبون بواسطة المعلومات المقدمة من المخدم بالتحقق من هوية المخدم ، في حال عدم نجاح العملية يتم قطع الاتصال، أما في حال نجاحها ينتقل الزبون إلى الخطوة رقم 4 .

4. يستخدم الزبون كافة المعلومات المتوفرة في المصافحة في توليد المفتاح الأساسي الأولي لهذه الجلسة ويقوم بإرساله إلى المخدم مشفرا بواسطة المفتاح العام للمخدم .

5. في حال طلب المخدم التحقق من هوية الزبون يقوم الزبون بوضع توقيعه الرقمي على البيانات المولدة عشوائيا من المخدم ويرسلها مع الشهادة الرقمية في نفس الرسالة التي يرسل فيها المفتاح الأساسي الأولي.

6. إذا كان المخدم قد طلب التحقق من هوية الزبون، فإنه يقوم بالتحقق من المعلومات المرسلة من الزبون وفي حال نجاح ذلك يقوم المخدم بفك تشفير المفتاح الأساسي الأولي بواسطة مفتاحه الخاص ومن ثم ينفذ المخدم والزبون عدد من العمليات كل على حده باستخدام نفس المفتاح الأساسي الأولي وذلك لتوليد المفتاح السري الأساسي .

7. بعد توليد المفتاح السري الأساسي لدى كل من المخدم والزبون، يقوم الطرفان باستخدامه في توليد مفاتيح الجلسة والتي سوف تستخدم لاحقا في تشفير وفك تشفير الرسائل بالإضافي إلى كشف محاولات العبث بها .

8. يرسل الزبون رسالة إلى المخدم يخبره فيها بأنه سوف يستخدم مفاتيح الجلسة في تشفير الرسائل القادمة ومن ثم يرسل رسالة تدل على انتهاء عملية المصافحة من جانبه، ولكنه يستمر في استقبال رسائل المخدم .

9. يرسل المخدم رسالة إلى الزبون يخبره فيها باستخدامه لمفاتيح الجلسة في تشفير الرسائل القادمة ومن ثم يرسل رسالة تدل على انتهاء عملية المصافحة .

أصبح من الممكن الآن بدء إرسال واستقبال المعلومات من كلا الطرفين [9].

5.3.3.3 التحقق من هوية المخدم

تمنع عملية التحقق من هوية المخدم انتحال الشخصية، حيث يقوم الزبون بطلب الشهادة الرقمية للمخدم، عند إرسال المخدم لشهادته الرقمية يسأل الزبون نفسه الأسئلة التالية والتي يجب أن يكون جواب كل منها " نعم " حتى يتم نجاح التحقق من هوية المخدم.

6.3.3.3 التحقق من هوية الزبون

يرسل المخدم طلب تحقق من هوية الزبون عند الحاجة لذلك ، ويرد الزبون بتشفير المعلومات التالية

بمفتاحه الخاص :

- الشهادة الرقمية للزبون .
- التوقيع الرقمي لبيانات معروفة من قبل المخدم والزبون فقط ويكون قد تم الاتفاق عليها خلال عملية المصافحة .

وبعد تشفير ما سبق يقوم الزبون بإرسالها إلى المخدم الذي يقوم بالتحقق من الشهادة بالطريقة التالية ، يجب أن يتم الرد بالإيجاب على أول أربعة أسئلة من الأسئلة التالية :

1. هل المفتاح العام للزبون يحقق توقيعه الرقمي ؟

يقوم المخدم بفك تشفير التوقيع الرقمي بواسطة المفتاح العام المرسل مع شهادة الزبون الرقمية ، فإذا وجد أن المعلومات المرسلة قد تغيرت فهذا يعني أن هناك من قام بتغيير البيانات بعد تطبيق التوقيع الرقمي عليها ، عدم تغير البيانات يبين وجود علاقة بين المفتاح العام المستخدم في فك التشفير والمفتاح الخاص المستخدم في التشفير ، إن اجتياز هذا الشرط لا يعني أنه تم إجازة الشهادة الرقمية وإنما يجب التحقق من الأسئلة الثلاثة الباقية لمنع حدوث انتحال شخصية حيث أنه ن الممكن أن يقوم شخص ما بإنشاء شهادة ما بهدف الوصول إلى موارد لا يحق له الوصول إليها .

2. هل تاريخ اليوم ضمن فترة صلاحية الشهادة ؟.

في حال كان الجواب لا، يتم إنهاء عملية التحقق عند هذا الحد وإعادة رسالة خطأ .

3. هل مصدر الشهادة الرقمية هو CA موثوق أي مصدر شهادات موثوق بالنسبة للمخدم ؟.

يملك كل مخدم SSL قائمة لمصدري الشهادات الموثوقين بالنسبة إليه ، تحتوي هذه القائمة على حقل DN(Distinguished Name) يحوي الاسم المميز لمصدر الشهادة ، يتم فحص هذا الشرط بالبحث عن مصدر شهادات موثوق في القائمة المخزنة لدى المخدم يتطابق حقل DN لديه مع حقل DN الموجود في الشهادة ، في حال تجاوز هذا الشرط يتم الانتقال إلى السؤال الرابع .

4. هل المفتاح العام العائد لمصدر الشهادة يفك تشفير التوقيع الرقمي ، وهل المعلومات المرسلة في الشهادة تتناقض مع التوقيع ؟.

للتحقق من التوقيع الرقمي يقوم المخدم بالخطوات التالية :

I. يفك الزبون شيفرة التوقيع الرقمي للجهة المصدرة CA بواسطة المفتاح العام الذي من المفترض وجوده في قائمة مصدري الشهادات الموثوقين .

II. يطبق المخدم تابع الاتجاه الواحد المستخدم من قبل CA المصدرة للشهادة على البيانات المرسلة من المخدم ، يتم بعد ذلك المطابقة بين التوقيع الرقمي المرسل مع الشهادة وقيمة التابع الناتجة :

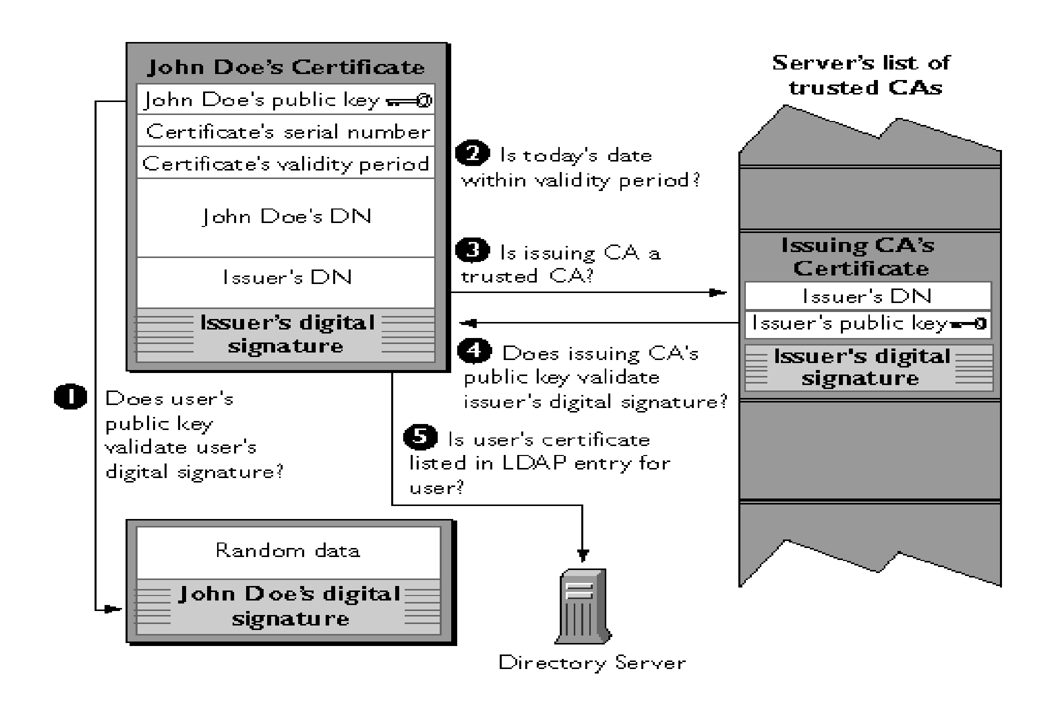
- ✓ في حال التطابق نستنتج أن المعلومات المرسلة في الشهادة صحيحة وفي هذه الحال يكون قد تم التحقق من شهادة الزبون الرقمية ويستطيع الطرفان البدء بتبادل المعلومات بينهما أو بإكمال التحقق من الشروط الاختيارية الباقية والتي ليست من التقنية الأساسية لـ SSL .
- ✓ ينتج عدم التطابق إما بسبب تغيير في الشهادة أو أن المفتاح العام المستخدم في فك التشفير لا يتوافق مع المفتاح الخاص المستخدم في تشفير المعلومات ، وفي هذه الحالة يتم رفض الشهادة .

5. هل الشهادة الرقمية للزبون موجودة في دليل LDAP(Lightweight Directory Access Protocol) ؟

دليل يمكن تعريف الدليل في حالتنا هذه على أنه نمط خاص من قاعدة البيانات يعطي إمكانية الوصول السريع لمخازن البيانات ، ويساعد هذا النمط في تنظيم مجموعات المستخدمين للموارد التي يقدمها المخدم حيث يعرف الصلاحيات الممنوحة لكل مجموعة ، في حال عدم وجود مدخل لشهادة ما في هذا الدليل فهذا يعني أن الشهادة ملغية ، في الحالة الأخرى يتم الانتقال إلى السؤال السادس .

6. إذا وجد مدخل للشهادة في الدليل فهل يملك الزبون ملك الشهادة الصلاحيات التي تمكنه من استخدام الموارد المطلوبة ؟

في حال الإجابة بنعم يقوم المخدم بتأسيس اتصال مع الزبون وبدء تبادل المعلومات أما في الحالة الأخرى يتم رفض طلب الزبون ، يبحث المخدم عن الصلاحيات الممنوحة للزبون في قوائم التحكم بالدخول ACLs (Access Control Lists) .



شكل(3.3): يوضح التحقق من هوية الزبون

4.3.3.أمن طبقة النقل(TLS) Transport Layer Security

وهي تقنية مطورة من سابقتها طبقة مآخذ التوصيل الآمنة (SSL)، وبروتوكولات التشفير التي توفر أمن الاتصالات عبر الإنترنت TLS وتشفير SSL لقطاعات من شبكة الاتصالات فوق طبقة النقل، وذلك باستخدام مفتاح التشفير غير المتناظر، و التشفير المتناظر للخصوصية، ورموز الرسائل لسلامة الرسالة إصدارات عديدة من البروتوكول قيد الاستخدام على نطاق واسع في التطبيقات مثل تصفح الإنترنت والبريد

الالكتروني والفاكس ، والرسائل الفورية والصوت عبر بروتوكول الإنترنت فويب.
TLSهو أحد معايير IETF للبروتوكولات، آخر تحديث في RFC 5246، ويقوم على أساس المواصفات التي وضعتها في وقت سابق SSL.

بروتوكول TLS يسمح بخدمة العملاء لتطبيقات الاتصال عبر الشبكة بطريقة تهدف إلى منع التنصت والعبث.
ويمكن استخدام معظم البروتوكولات سواء مع أو بدون TLS (أو SSL) من الضروري أن نشير إلى الخادم ما إذا كان العميل يجري اتصال TLS أو لا.

هناك طريقتان رئيسيتان لتحقيق ذلك، الأولى هي استخدام رقم منفذ مختلف لاتصالات TLS (على سبيل المثال المنفذ 443 لHTTPS). والأخرى هي استخدام رقم المنفذ العادي ويكون طلب العميل أن الملقم تبدل اتصال TLS باستخدام آلية محددة في البروتوكول (على سبيل المثال STARTTLS لبروتوكولات البريد والأخبار).

مرة واحدة العميل والخادم قد قررا استخدام TLS إجراء تفاوض لاستخدام إجراء المصافحة. وخلال هذه المصافحة، العميل والخادم يتفقان على معايير مختلفة تستخدم لإرساء اتصال امن[24].

1.4.3.3 المصافحة في TLS

1. المصافحة تبدأ عندما يتصل عميل إلى خادم TLS لتمكين طلب اتصال آمن، ويقدم قائمة من برامج التشفير معتمدة (الأصفار ووظائف التجزئة).

من هذه القائمة، الخادم يختار أقوى الشفرات، وظيفة التجزئة أنها تدعم أيضا إعلام العميل بهذا القرار.

2. يرسل الملقم مرة أخرى تحديد هويته في شكل شهادة رقمية. الشهادة عادة ما تحتوي على اسم الخادم، ومصدق موثوق به (CA)، ومفتاح للملقم التشفير العامة.

العميل يمكنه الاتصال بالخادم الذي أصدر الشهادة ، والتأكد من صلاحية الشهادة قبل المتابعة.

3. من أجل توليد مفاتيح الجلسة المستخدمة للاتصال آمن، يقوم العميل بتشفير رقم عشوائي مع مفتاح للملقم العام ويرسل النتيجة إلى الملقم. فقط يجب أن يكون الملقم قادرا على فك تشفيرها، مع المفتاح الخاص من الرقم العشوائي، وكلا الطرفين تولد مادة المفتاح لتشفير وفك، هذا ويختتم مصافحة ويبدأ اتصال آمن، والذي يتم فيه تشفير و فك التشفير مع المواد الأساسية حتى يغلق الاتصال[24].

إذا أي واحدة من الخطوات المذكورة أعلاه فشلت، فان مصافحة TLS ستفشل ولن يتم إنشاء اتصال آمن.

IPSec .5.3.3

IPSec: هي مجموعة معايير من البروتوكولات والخوارزميات طورت بواسطة اللجنة الخاصة بنظام الإنترنت (IETF) Internet Engineering Task Force واعتمدت كمعايير الإنترنتِ لتوفر التحقق من سلامة وسرية المعلومات التي أرسلت عبر شبكات IP، وذلك بجعلها تعمل في طبقة IP بحيث تتمكن من حماية أي نوع من نقل البيانات من خلالIP [11].

عادةً يعبر عن IPSec بأنها Transparent Security Protocol لأن المستخدم و التطبيقات لا يشعرون بوجودها لأنها تعمل على طبقة الشبكة (Network Layer)، ويعمل IPSec في البيئات التي تكون سرعة الاتصال سريعة.

Application	S/MIME	PGP		
Presentation				
Session	Kerberos	HTTP	UDP	SSL
Transport	TCP			
Network	IP			IPsec
Data Link				
Physical				

شكل (4.3): توضح الصورة موقع IPSec في OSI Model

1.5.3.3 بروتوكولات IPSec

ينقسم IPSec إلى ثلاث بروتوكولات:

أولاً: AH : Authentication Header

يستخدم AH في توقيع Sign الرسائل والبيانات ولا يعمل على تشفيرها Encryption ، حيث يحافظ على:

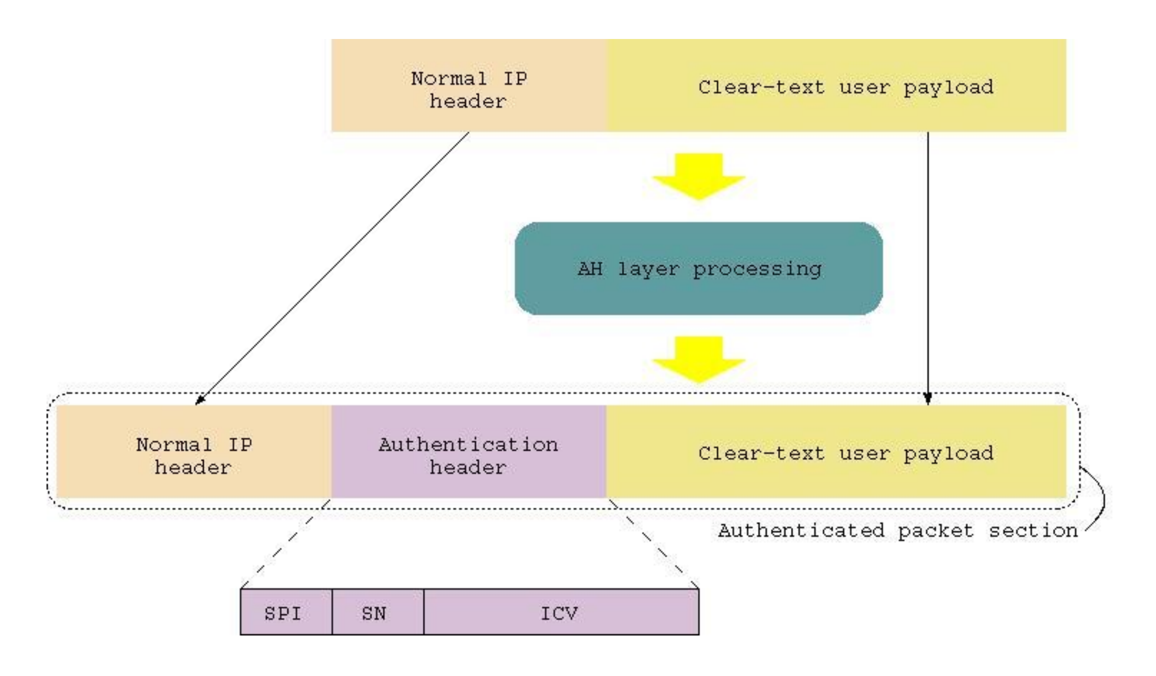
1. موثوقية البيانات Data authenticity: أي أن البيانات المرسلة من هذا المستخدم هي منه وليست مزورة أو مدسوسة.

2. صحة البيانات Data Integrity : أي أن البيانات المرسلة لم يتم تعديلها على الطريق (أثناء مرورها على الأسلاك) .

3. عدم إعادة الإرسال Anti–Replay: وهذه الطريقة التي يستخدمها المخترقون حيث يقومون بسرقة كلمة المرور وهي مشفرة ويقومون بإعادة إرسالها في وقت آخر للسيرفر وهي مشفرة يفك السيرفر التشفير ويدخل اسم المستخدم على أنه شخص آخر، IPSec يقدم حلولاً لمنع هذه العملية من الحدوث.

4. الحماية ضد الخداع Anti–Spoofing protection : يوفرIPSec حماية ضد الخداع من قبل المستخدمين ، مثلاً يمكن أن يحدد مدير الشبكة انه لا يسمح لغير المستخدمين على subnet 192.168.0.X بينما لا يسمح لحاملي الهوية 192.168.1.x من دخول السيرفر، فيمكن للمستخدم أن يغير IP Address الخاص به ، لكن IPSec يمنع ذلك .(وأيضا يمكنك القياس على ذلك من خارج الشبكة إلى داخلها) يكون لكل حزمة Packet موقعها Digitally signed.

هذا هو الشكل العام لحزمة البيانات Packet التي تمر في بروتوكول AH .



شكل(5.3): يوضح حزمة البيانات Packet التي تمر في بروتوكول AH

ثانياً: ESP : Encapsulating Security Payload

يوفر هذا البروتوكول التشفير والتوقيع للبيانات معا Encryption and Signing ، و يستخدم هذا البروتوكول في كون المعلومات سرية Confidential أو Secret ، أو عند إرسال المعلومات عن طريق Public Network مثل الانترنت.

يوفر ESP المزايا التالية:

1.Source authentication : وهي مصداقية المرسل، حيث لا يمكن لأي شخص يستخدم IPSec تزوير هويته (هوية المرسل).

2.التشفير للبيانات Data Encryption : حيث يوفر التشفير للبيانات لحمايتها من التعديل أو التغيير أو القراءة.

3.Anti-Replay : موضحة في AH .

4.Anti-Spoofing Protection : موضحة في AH.

ثالثاً : Internet Key Exchange : IKE

الوظيفة الأساسية لهذا البروتوكول هي ضمان الكيفية وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي IPSec ، فهو بروتوكول negotiation أي النقاش في نظام IPSec كما أنه يعمل على تأكيد طريقة الموثوقية Authentication والمفاتيح الواجب استخدامها ونوعها حيث IPSec يستخدم التشفير DES3 وهو عبارة عن زوج من المفاتيح ذاتها يتولد عشوائياً بطرق حسابية معقدة ويتم إعطاءه فقط للجهة الثانية ويمنع توزيعه وهو من نوع Symmetric Encryption أي التشفير المتوازي ويستخدم تقنية Private Key .

2.5.3.3 أنظمة IPSec المستخدمة في حماية الشبكات:

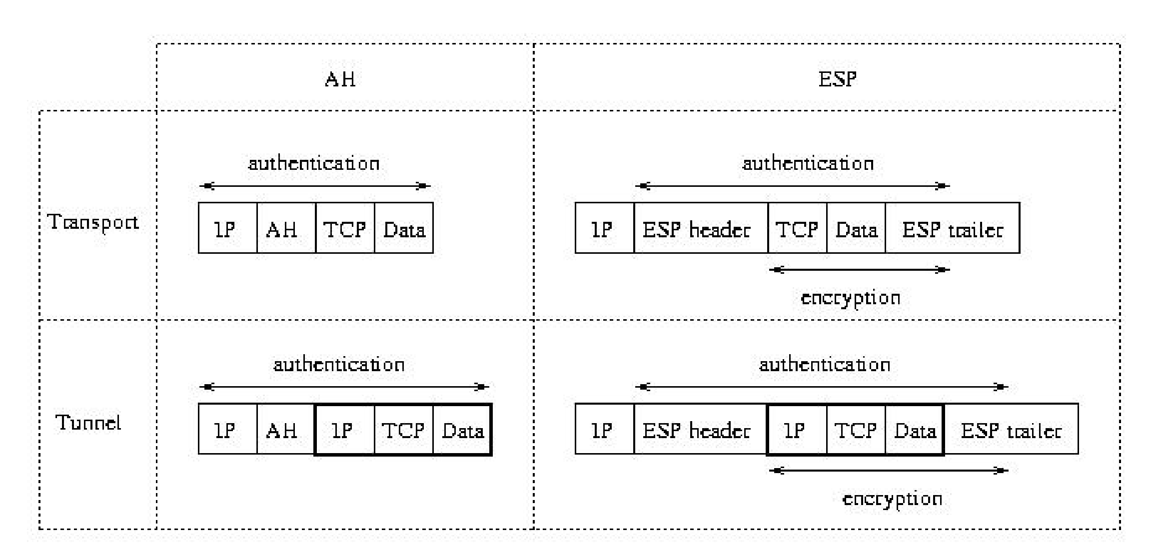
1. نظام النقل Transport Mode
2. نظام النفق Tunnel Mode [3].

1.2.5.3.3 نظام النقل Transport Mode: يستخدم الشبكة المحلية LAN حيث يقدم خدمات التشفير للبيانات التي تتطابق والسياسة المتبعة في IPSec بين أي جهازين في الشبكة أي يوفر Endpoint-to-Endpoint Encryption إذا قمنا بضبط سياسة IPSec على تشفير جميع الحركة التي تتم على بورت 23 وهو بورت Telnet (حيث Telnet ترسل كل شيء دون تشفير Plaintext) فإذا تمت محادثه بين السيرفر والمستخدم على هذا البورت فان IPSec يقوم بتشفير كل البيانات المرسلة من لحظة خروجها من جهاز المستخدم إلى لحظة وصولها إلى السيرفر، يتم تطبيق هذا النظام في الحالات التالية:

أولاً: المحادثة تتم بين الأجهزة في داخل أو نفس الشبكة الداخلية الخاصة Private LAN.
ثانياً: المحادثة تتم بين جهازين ولا يقطع بينهما Firewall يعمل عمل NAT : Network Address Translation نظام يمكن Firewall من استبدال جميع عناوين IPs في الشبكة الداخلية من حزمة البيانات Packet واستبدالها في عنوان Public IP آخر، ونستفيد من ذلك أنه لن نحتاج سوى عنوان IP واحد One Public IP ، وأيضاً يقوم بإخفاء عناوين الأجهزة عن شبكة الانترنت للحماية من الاختراق الخارجي .

2.2.5.3.3 نظام النفق Tunnel Mode: يتم استخدام هذا النظام لتطبيق IPSec بين نقطتين تكون بالعادة بين 2 Routers، إذاً يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافياً أي سيتم قطع الانترنت في طريقها إلى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعدة جغرافيا WAN، يستخدم هذا النظام عند الحاجة لتأمين البيانات فقط أثناء مرورها من مناطق غير آمنة كالانترنت، فمثلاً إذا أراد فرعين لشركة أن يقوم بتشفير جميع البيانات التي يتم إرسالها فيما بينهم على بروتوكول FTP فيتم إعداد IPSec على أساس Tunneling Mode .

وهذه صوره مخطط لكل من Packets في AH، ESP في كلا النظامين Tunnel and Transport Modes .



شكل(6.3):مخطط Packets في AH ، ESP في النظامين Tunnel and Transport Modes .

3.5.3.3 ميزات IPSec

لقد ظهر ضعف كبير في عملية Encryption العادية التي تتم بين الأجهزة في الشبكات، وهذا الضعف تمثل في صعوبة تطبيق هذا الموضوع، وأيضا استهلاكه للوقت أي بطوء الشديد في القيام بعملية التشفير وفكه Encryption and decryption، فالفائدة الكبرى التي ظهرت في IPSec هي أنه يوفر حماية كاملة وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالث Layer 3 of the OSI Model وما بعدها.

من مميزات IPSec أيضا هو أنه موجود أصلاً Built–in في داخل حزمة IP Packet، فلذلك هو لا يحتاج لأي إعدادات لانتقاله عبر الشبكة ولا يحتاج لأي أجهزة إضافية لذلك [14].

4.5.3.3 طرق IPSec في حماية الشبكة

البيانات التي تمر في الشبكة يمكن أن تتعرض للعديد من أنواع الهجمات المختلفة، بعض الهجمات تكون غير فعاله Passive مثل مراقبة الشبكة Network Monitoring، وبعضها فعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر أسلاك الشبكة. و سوف نستعرض بعض أنواع الهجمات على الشبكات.

أولاً: التقاط حزم البيانات Eavesdropping:حيث يتم بذلك مراقبة حزم البيانات التي تمر عبر الشبكة بنصها الواضح دون تشفير Plain text والتقاط ما يريد منها، ويعالجها IPSec عن طريق تشفير حزمة البيانات، حتى لو التقطت الحزمة فإن الفاعل لن يستطيع قراءتها أو العبث بها، لأن الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل.

ثانيا: تعديل البيانات Data modification:حيث يتم بذلك سرقة حزم البيانات من الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل، ويقوم IPSec بمنع ذلك عن طريق استخدام الهاش Hash ووضعه مع البيانات ثم تشفيرها معاً ، وعندما تصل الحزمة إلى الطرف المستقبل فإن الجهاز يفحص Checksum التابع للحزمة إذا تمت مطابقته أم لا، فإذا تمت المطابقة مع الهاش الأصلي المشفر تبين أن الحزمة لم تعدل، لكن إذا تغير الهاش فإن حزمة البيانات قد تم تغييرها على الطريق.

ثالثاً: انتحال الشخصية Identity spoofing: بحيث يتم استخدام حزم البيانات على الشبكة والتقاطها وتعديلها لتبين هوية مزورة للمرسل، أي خداع المستقبل بهوية المرسل، ويمنع ذلك عن طريق الطرق الثلاث التي يستخدمها IPSec وهي: بروتوكول الكيربرس (Kerberos Protocol)، والشهادات الالكترونية Digital Certificates، ومشاركة مفتاح معين (Preshared Key).

حيث لا تتم عملية بدأ المحادثة وإرسال البيانات قبل التأكد من صحة الطرف الثاني عن طريق إحدى الطرق المذكورة.

رابعاً: DoS –Denial of Service رفض الخدمة أو حجبها: حيث تعمل هذه الهجمة على تعطيل خدمة من خدمات الشبكة للمستخدمين والمستفيدين منها، مثلاً كإشغال السيرفر في الشبكة بعمل عليه Flood مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين. ويعمل IPSecعلى منع ذلك عن طريق إمكانية غلقه أو وضع قواعد للمنافذ المفتوحة Ports.

خامساً: MITM –Man In The Middle: من أشهر الهجمات في الشبكات، وهي أن يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسلة من طرف لآخر وإمكانية العمل على تعديلها أو العمل على عدم إيصالها للجانب الآخر، ويعمل IPSec على منعه بواسطة طرق التحقق من الموثوقية Authentication methods .

سادساً: الهجمات على طبقة التطبيقات Application Layer Attacks : حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في أجهزة الشبكة وأيضاً تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الأمثلة عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى أخطاء المستخدمين. يعمل IPSec على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أي حزمة بيانات لا تتطابق مع الشروط الموضوعة لذلك ، لذا تعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج [3][19].

بشكل عام IPSec يحمي من معظم الهجمات عن طريق استخدامه ميكانيكية التشفير المعقدة، حيث يوفر التشفير الحماية للبيانات والمعلومات أيا كانت أثناء انتقالها على الوسط (أيا كان) عن طريق عمليتي التشفير Encryption والهاش Hashing[14].

طريقة التشفير المستخدمة في IPSec عبارة عن دمج لعدة Algorithms ومفاتيح، وحيث

Algorithm: عبارة عن العملية الحسابية التي تمر فيها البيانات لكي تشفر.

Key : وهو عبارة عن رقم (كود) سري يتم من خلاله قراءه أو تعديل أو حذف أو التحكم في البيانات المشفرة بشرط مطابقته للطرف الثاني الذي قام بعملية التشفير[3][19] [20].

SMB.6.3.3

وهي SMB Signing اختصار Server Message Block وهي packets التي يتم إرسالها بين السيرفر والأجهزة في عملية المشاركة في الملفات وغيره Sharing، وللحماية من طريقة سرقة المعلومات أثناء مرورها في الأسلاك Man In The Middle MITM وهذه الطريقة تدعى SMB Signing يتم بواسطتها إضافة Hash وهي طريقة يتم من خلالها استخلاص رمز معين حسب حسابات رياضيه من الرسالة ، ومن الأمثلة عليهMD4، MD5 ، SHA-1 ويتم تشفير هذا Hash وإضافته للرسالة وبذلك نحافظ على صحة الرسالة Message or Packet Integrity [17].

7.3.3.الهاش HASH

الهاش عبارة عن مجموعة أرقام وأحرف عشوائية يتم توليدها بطرق حسابيه معقده جدا من نص (ممكن رسالة) أو من حزمة بيانات، أو حتى من بيانات حجمها 1000 ميجا، الهاش طوله وشكله ثابت لا يتغير، هو لا يشفر، وإنما هو للحفاظ على مصداقية البيانات.

بمعنى انه إن أراد احد إرسال رسالة، فانه يخرج الهاش الخاص بها و يرسله مع الرسالة، و الشخص الذي يستقبل الرسالة يقارن الهاش الذي استلمه بالهاش الخاص بالرسالة, فان تم تعديل الرسالة و لو بإضافة مسافة، فان الهاش سيختلف.

يستخدم الهاش في برامج Open Source بكثرة ، لأنه يمكن تعديلها و نسبها للشركة الأم (هذا هو MD5 الموجود في مواقع اللينكس) .

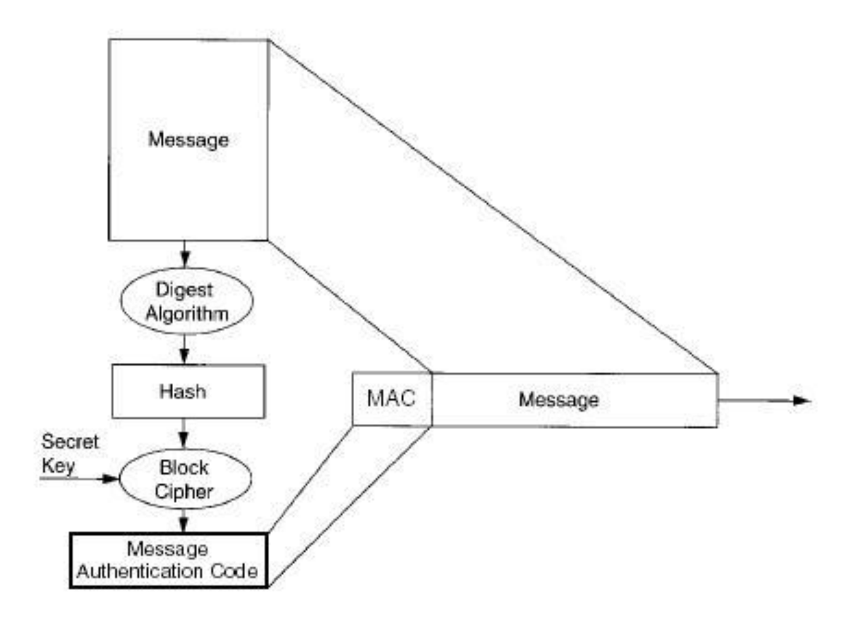
الهاش من أنواعه القديمة : Message Digest 4 :MD4 تم فكه بطريقة Birthday Attack ومن أنواعه الجديدة والمستعملة بكثرة Message Digest 5 : MD5 لكن يقال أيضا انه تم كسره عن طريق CIA وان جميع لجان الاتحاد الأوروبي لم تعد تستعمله.

أحدث أنواعه وأقواها هو SHA-1 -Secure Hash Algorithm وهو المستخدم في متصفح IE . مع العلم أن الهاش One way process بمعنى انه لا تستطيع إرجاع شيء من الهاش المنتج.

1.5.3.3 تلخيص وتشويش الرسالة: Message Digesting and Hashing

من خلال ما تم ذكره سابقا يمكننا القول بأنه عند القيام بعملية التشفير فإن عمليتين أساسيتين يتم تنفيذهما الأولى : تشفير محتويات الرسالة لمنع الوصول لمحتواها الثانية التأكد من سلامة البيانات التي تم تشفيرها وبالتالي التأكد من عدم حدوث أي عملية تعديل على هذه البيانات .

وتسمى هذه الطريقة بـ (digest) والتي يتم من خلالها أخذ الرسالة الطويلة وتحويلها إلى شفرة نصية قصيرة ، وهذه العملية وحيدة الاتجاه أي لا يمكن استرداد البيانات بعد تحويلها باستخدام توابع التلخيص (digest) وبعد ذلك يتم تشفير هذه السلاسل النصية القصيرة مما يسرع من عملية التشفير باعتبار أن النص المخرج هو نص صغير نسبيا ونحصل ما يدعى " رمز توثيق الرسالة " والذي يتم إضافته للرسالة قبل إرسالها كما هو الحال في الصورة التالية



شكل(7.3): يوضح توثيق الرسالة

يجب أن يحتوي أي نظام تشويش (Hashing) جيد على ميزتين أساسيتين:

1. أن يكون من الصعب جدا عكسه (أي استعادة النص بعد أن تم تطبيق التوابع عليه).

2. صعوبة التكرار أي أنه من الصعب جدا أن يتم تطبيق التوابع على رسالتين مختلفين وإعطاء الخرج نفسه.

وأكثر خوارزميتين مستخدمتين في هذا المجال هما (MD5،SHA) ، و اللتان وجدتا طريقهما إلى بروتوكولات الدفع الالكتروني.

MD5.1 :

خوارزمية (MD5) هي جزء من مجموعة خوارزميات (متضمنة MD2, MD4) تم تطويرها من قبل Rone Rivest وتقوم خوارزمية MD5 على إضافة حقل طول للرسالة ومن ثم تبطين هذا الحقل ضمن عدة أجزاء من الكتل حجم الكتلة منها هو 512 بت.

يقوم التشويش بإخراج سلسلة من القيم ذات حجم 128 بت مستخرجة من معالجة الكتلة الأخيرة من الرسالة.

2. خوارزمية التشويه المحمية The Secure Hash Algorithm (SHA) :

قام المعهد الوطني للمعايير القياسية والتقنيات (NIST) بإصدار سلسلة من المعايير القياسية في عام 1993 م إحداها تحدد خوارزمية التشويش المحمية (SHA) وهي تعتمد بشكل كبير جدا على عمل (Rone Rivest) في خوارزمية (MD5). تعمل خوارزمية التشويه المحمية على أربع مراحل كما هو الحال في (MD) إلا أن هذه المراحل أكثر تعقيدا. إن خرج الرسالة الملخصة هو 160 بت والذي هو عبارة عن سلسلة من القيم التي يتم انتقالها من مرحلة إلى أخرى والتي هي بطول 160 بت أيضا[28].

8.3.3. أنظمة كشف التطفل: IDS (Intrusion detection systems)

معظم المنشآت سواء كانت صغيرة أو كبيرة تحتاج إلى جهاز إنذار ضد السرقة للحفاظ على المعلومات القيّمة لديها ، وقد ظهر نظام جديد يغني عن أجهزة الإنذار ويؤدي وظيفتها على أكمل وجه وهو ما يعرف بنظام كشف التطفل الذي هو في جوهره نظام إنذار ضد السرقة ، يعمل على مراقبة الشبكة وإصدار إنذارات فيما إذا شك بأن الشبكة تتعرّض للهجوم في وقت ما.

يوجد آليتان لكشف التطفل:

الكشف عن الوضع الشاذ:(Anomaly detection)

هذه الطريقة مبنية على أساس مراقبة سلوك المستخدمين في النظام الاعتيادي وتخزين السلوك في النظام ، فهي تقوم على أساس مقارنة السلوكيات مع الحزم الإلكترونية لاكتشاف الانحرافات، و من أبرز مساوئ هذه الآلية صدور إنذارات إيجابية خاطئة (False Positive Alarms)نتيجة اكتشاف هجمات غير معرّفة.

الكشف عن الإساءة:(Misuse detection)

تعتمد على مقارنة الصفات المتعلقة بالحزم مع الصفات المخزنة في قاعدة البيانات، و من أبرز مساوئ هذه الآلية هو انحصارها فقط على الهجوم المعروف في قاعدة البيانات[29].

9.3.3.الجدار الناري (Firewall)

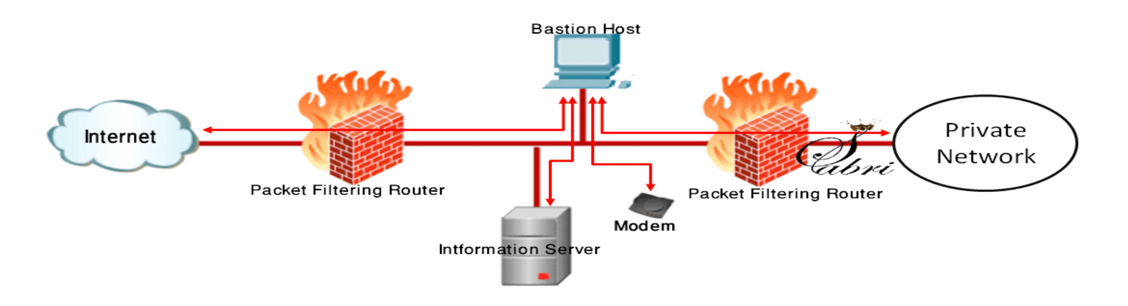
هو جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يقرر أحقية المرور ضمناً لقواعد معينة[3].

ظهرت تقنية الجدار الناري في أواخر الثمانينات عندما كانت الإنترنت تقنية جديدة نوعاً ما من حيث الاستخدام العالمي. الفكرة الأساسية ظهرت استجابة لعدد من الاختراقات الأمنية الرئيسية لشبكة الإنترنت التي حدثت في أواخر الثمانينات[12].

1.9.3.3 وظيفته

وظيفة الجدار الناري داخل الشبكة هو منع اختراق الشبكات الخاصة، وفي الحالة الثانية يفترض به أن يحتوي ويؤخر المخاطر الموجود في بيئة معينه من الانتقال إلى بيئة أخرى[3].

من دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة. فممارسات الأمان المعيارية تحكم بما يسمى بمجموعة قوانين "المنع أولاً" للجدار الناري، الذي من خلاله يسمح بمرور فقط وصلات الشبكة المسموح بها بشكل تخصيصي، ولسوء الحظ فان إعداد مثل هذا يستلزم فهم مفصل لتطبيقات الشبكة ونقاط النهاية اللازمة للعمل اليومي للمنظمات، العديد من أماكن العمل ينقصهم مثل هذا الفهم وبالتالي يطبقون مجموعة قوانين "السماح أولاً"، الذي من خلاله يسمح بكل البيانات بالمرور إلى الشبكة ان لم تكن محددة بالمنع مسبقاً.



شكل(8.3): يوضح جدار النار

أول بحث نشر عن تقنية الجدار الناري كانت عام 1988، عندما قام مهندسون من (DEC) بتطوير نظام فلترة عرف باسم جدار النار بنظام فلترة العبوة، هذا النظام الأساسي يمثل الجيل الأول الذي سوف يصبح عالي التطور في مستقبل أنظمة أمان الإنترنت، تعمل فلترة العبوات بالتحقق من العبوات (packets) التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الإنترنت. إذا كانت العبوة تطابق مجموعة قوانين فلتر العبوة فإن النظام سيسمح بمرور العبوة أو يرفضها يتخلص منها ويقوم بإرسال استجابة "خطأ" للمصدر.

2.9.3.3 آلية عمل الجدران النارية:

هناك ثلاثة طرق تستند إليها الجدران النارية في آلية عملها:

I. تصفية الحزم: (Packet Filtering)

تنتقل المعلومات على هيئة حزم تمّر خلال الجدار النّاري الذي يقوم بدوره بفحصها والتحقق من موافقتها للشروط.

II. وكيل الخدمة: (Proxy Service)

يعيّن الجدار النّاري نفسه وكيلاً عن الشبكة الداخلية فيكون بذلك قد حجب عناوين الشبكة الداخلية وبالتالي يتّم إرسال البيانات إلى عنوان الجدار الناري الذي يقوم بدوره بتوجيهها إلى وجهتها الأصلية.

III. مراقبة السياق:(Stateful Inspection)

إن الجدار الناري هنا يقوم بفحص حقول معيّنة في الحزم فلا يفحص مكونات الحزم كلها بل يعمل على مقارنتها بالحقول المناظرة لها بنفس السياق (مجموعة الحزم الإلكترونية المتبادلة عبر شبكة الإنترنت) ، وعندما يكتشف أن حزم معينة لم تلتزم بقواعد السياق فإن ذلك دليل قاطع على وجود اختراق يهدّد أمن الموقع.

وهناك عدة معايير يمكن استخدامها لمعرفة فيما إذا كانت الحزم صحيحة وهي كالآتي[25]:

1. العنوان الرقمي: (IP Address)

هو رقم لكل مشترك على الشبكة العنكبوتية يوفّر للجدار الناري المقدرة على التحكم بالسماح أو المنع لمرور الحزم القادمة.

2. اسم النطاق: (Domain Name)

يتيح للجدار الناري منع مرور الحزم القادمة من نطاق معيّن.

3. بروتوكول التخاطب:(Protocol)

وهي طريقة للتخاطب وتبادل المعلومات بين العميل والمنشأة، أمّا بالنسبة للعميل فقد يكون شخص أو برنامج كالمتصفح(Browser).

تتعدّد هذه البروتوكولات و أبرزها ما يلي [26]:

- بروتوكول :HTTP يستعمل لتبادل المعلومات بين المتصفح وجهاز الخادم.
- بروتوكول: FTP يستخدم لنقل الملفات عوضاً عن إرسالها كمرفقات (Attachment) في البريد الإلكتروني.
- بروتوكول :SMTP يستعمل لنقل البريد الإلكتروني.
- بروتوكول :SNMP يستعمل لإدارة الشبكات وجمع المعلومات.
- بروتوكول :Telnet يستعمل للتحكم بالجهاز عن بعد.

3.9.3.3 جدار النار لطبقة التطبيقات (Application Layer Firewall)

الفائدة الرئيسية من الجدار الناري لطبقات التطبيقات أنه يمكن أن "يفهم "بعض التطبيقات والأنظمة مثل نظام نقل الملفات "DNS" تصفح المواقع ويمكنه أن يكتشف إذا ما كان هنالك نظام غير مرغوب فيه يتم تسريبه عبر مرافئ غير اعتيادية أو إذا كان هنالك نظام يتم إساءة استخدامه بطريقة مؤذية ومعروفة.

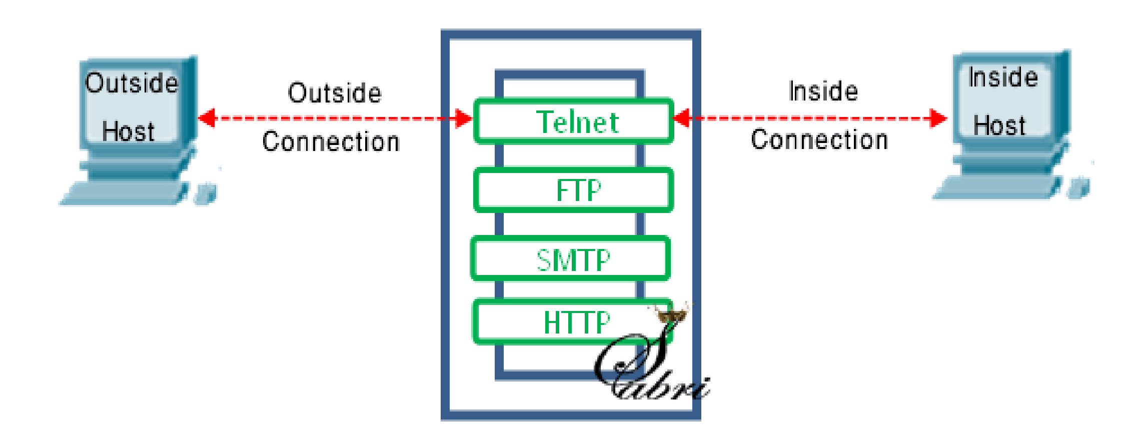
وظيفة: التحقق العميق للعبوة الحالية للجدران الحديثة يمكن مشاركتها مع أنظمة منع الاختراق.(IPS)

تعمل الجدران النارية لطبقات التطبيقات على مستوى التطبيق لفئة "TCP\IP"مثل جميع أزمة المتصفح، أو جميع أزمة "TELNET" و"FTP"، ويمكن أن يعترض جميع العبوات المنتقلة من وإلى التطبيق)، ويمكن أن يحجب العبوات الأخرى دون إعلام المرسل عادة. في المبدأ يمكن لجدران التطبيقات النارية منع أي اتصال خارجي غير مرغوب فيه من الوصول إلى الأجهزة المحمية[22].

عند تحري العبوات جميعها لإيجاد محتوى غير ملائم، يمكن للجدار الناري أن يمنع الديدان (worms) والأحصنة الطروادية (Trojan horses) من الانتشار عبر الشبكة. ولكن عبر التجربة تبين أن هذا الأمر يصبح معقدا جداً ومن الصعب تحقيقه (مع الأخذ بعين الاعتبار التنوع في التطبيقات وفي المضمون المرتبط بالعبوات) وهذا الجدار الناري الشامل لا يحاول الوصول إلى مثل هذه المقاربة.

الحائط الناري XML يمثل نوعاً أكثر حداثة من جدار طبقات التطبيقات الناري.[21]

4.9.3.3 مستوى منفذ التطبيقات Application-Level Gateway



شكل(9.3): منفذ التطبيقات

أو ما يسمى Proxy Server حيث يعمل كمنظم للطبقة السابعة من (Application Layer) OSI حيث يخرج المستخدم للعالم الخارجي عن طريق Gateway باستخدام تطبيقات TCP/IPمثل FTP، Telnet حيث Gateway تسأل المستخدم الذي يريد الاستفسار عن اسم المستخدم و كلمة المرور للمصادقة لكي يتم إكمال الاتصال و حينها تتطابق بالصواب فإن الاتصال يتم فإذا كانت الخدمة لم يتم تعريفها في Proxy server فإن الاتصال أو الخدمة المطلوبة لن يتم إتمامها و من هذه الخاصية فإن مدير الشبكة يستطيع السماح فقط للخدمات التي يريد تداولها و استخدامها و منع الأخرى . يميز هذه الطريقة هو أنها تسمح بمراقبة و تسجيل كل ما يحصل في كل التطبيقات العليا و السفلى[23].

من أشهر المنظمات المنتجةFirewall Linux: ، Cisco ،Microsoft ، Juniper

10.3.3.المنطقة المحايدة (DMZ) Demilitarized Zone

أطلق مصطلح المنطقة المنزوعة السلاح على المنطقة الجغرافية المحايدة بين الأطراف المتنازعة، وصار هذا المصطلح يستخدم في شبكات الحاسب للدلالة على المنطقة الشبكية الفاصلة والمحايدة بين شبكة المنظمة الخاصة والشبكة العالمية كوسيلة لحماية شبكة المنظمة.

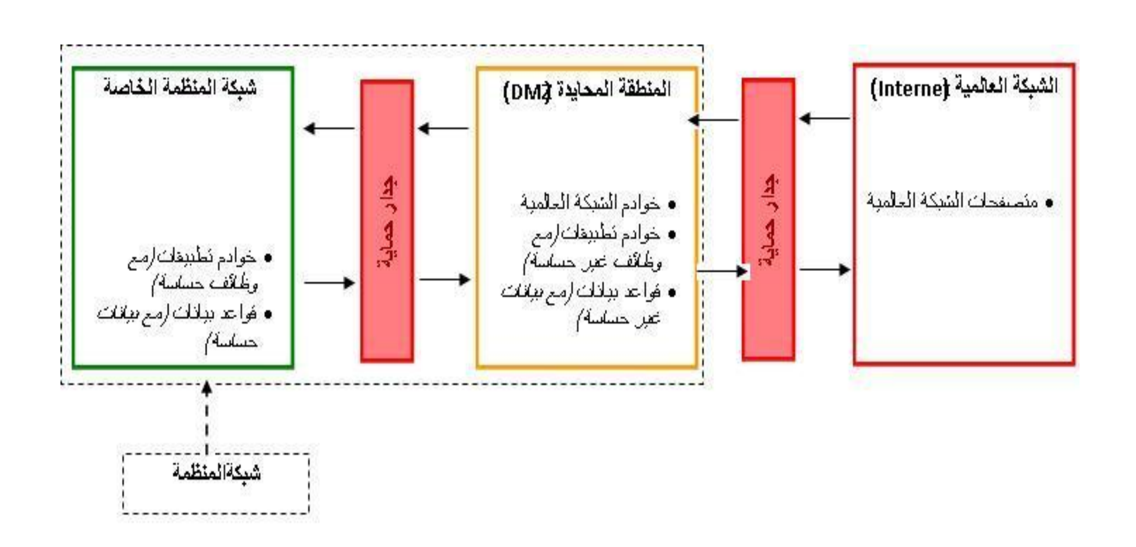


شكل(10.3): المنطقة المنزوعة السلاح بين الكوريتين الشمالية والجنوبية – الشريط الأبيض الفاصل

1.10.3.3 تعريف

يعتبر التصميم المادي للشبكة (Network Topology) من العوامل الأساسية لأمن الشبكات، وحتى لو تم تعديل هذا التصميم لأسباب أمنية، فإنها في النهاية لابد أن تعكس متطلبات المنظمة ومتطلبات مستخدميها، ومن هنا أتت فكرة مناطق الشبكة (Network Zones) [30].

المنطقة المنزوعة السلاح هي واحدة من هذه المناطق الشبكية والتي تستخدم لتقليل الأخطار المحتملة على شبكة المنظمة الخاصة من الاتصالات الغير المصرحة القادمة من الشبكة العالمية وبالتالي إمكانية تسرب بيانات المنظمة السريّة.



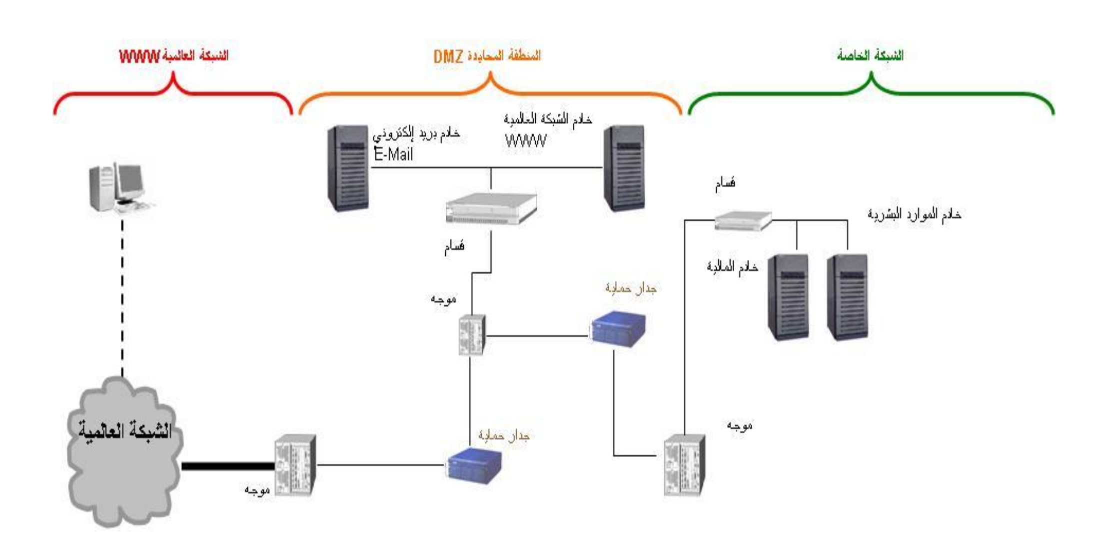
شكل (11.3): المنطقة المحايدة (تصميم منطقي)

كما نرى في الشكل أن بإمكان مستخدمي الشبكة العالمية من الاتصال بالمنطقة المحايدة من شبكة المنظمة لكن ليس بإمكانهم الدخول إلى شبكة المنظمة الخاصة.

في الشكل أيضا نرى جدارين ناريين، الهدف من الجدار الناري الأول بين الشبكة العالمية والمنطقة المحايدة من شبكة المنظمة هو حماية الخوادم الموجودة في المنطقة المحايدة – والتي بطبيعتها لابد أن تكون مرئية

للعالم – من الهجمات عن طريق الشبكة العالمية، وهذه الحماية بناءا على الفلترة كالسماح لبروتوكولات معينة بالمرور مثل (HTTPS،HTTP) ومنع البرتوكولات الأخرى مثل (Telnet،FTP).

والهدف من الجدار الناري الثاني بين المنطقة المحايدة والمنطقة الخاصة من شبكة المنظمة هو تزويد حاجز أمني مقوى لحماية المنطقة الخاصة، وأيضا كما في الجدار الثاني هذه الحماية بناءا على الفلترة كالسماح لبروتوكولات معينة بالمرور مثل (ODBC, JDBC) و يجب أن تكون الفلترة في هذا الجدار الناري مقيدة أكثر من الجدار الناري الأول، ففي حالة اختراق الجدار الناري الاول فإن احتمالية اختراق الجدار الناري الثاني أقل [30].



شكل(12.3): المنطقة المحايدة (تصميم فيزيائي)

الخوادم التي يجب وضعها في المنطقة المحايدة:

بشكل عام أفضل مكان للخوادم وقواعد البيانات المعدة للتعامل مع الشبكة العالمية هو منطقة الشبكة المحايدة، ومن الأمثلة على هذه الخوادم التالي:

- خوادم الشبكة العالمية (Web Servers)

- خوادم بروتوكول نقل الملفات (FTP Servers)
- خوادم الاتصال البعيد
- خوادم البريد الإلكتروني

إجراءات خاصة للمنطقة المحايدة:

- ✓ تقوية الخوادم من خلال فحص و تقليص الثغرات الأمنية، وذلك لأن المنطقة المحايدة عرضة للاختراقات القادمة من الشبكة العالمية.
- ✓ تعطيل الخدمات غير المستخدمة، مثل الحسابات الزائدة و خدمة نقل الملفات (FTP).
- ✓ عمل فحص و تدقيق دوري لأنشطة الخوادم.
- ✓ التأكد من تركيب آخر التحديثات للخوادم.
- ✓ التأكد من أن الخوادم مجهزة بالشكل الكافي و المطلوب.

تحديات المنطقة المحايدة

الأداء:بطء أداء الشبكة بسبب الزيادة في عدد الأجهزة والموجهات، وهذا لأن المنطقة المحايدة تعتبر تقنيا كشبكة فرعية ، وإنشاء شبكة فرعية يختلف عن التوسع في الشبكة نفسها.

الإدارة:ارتفاع تكلفة إدارة ومراقبة وصيانة الشبكة، و هذا ناتج عن إضافة شبكة فرعية.

المرونة: قد لا تتوافق جميع التطبيقات مع هذه المعمارية، فإضافة شبكة فرعية قد يتعارض مع معمارية شبكية تحد من الشبكات الفرعية.

2.10.3.3 تقنية أوعية العسل (Honey pots)

هي تقنية تستخدم في المناطق المحايدة لإبعاد الاختراقات المحتملة على شبكة المنظمة، و هي عبارة عن خوادم مزودة ببرامج و بيانات تظهر و كأنها موثوقة و صحيحة لتوجيه أنظار المخترقين إليها و صرفهم عن الخوادم الحقيقية.

فائدة أخرى من هذه التقنية ألا وهي إعطاء انطباع عن أساليب المخترقين للاستفادة منها في صد هجماتهم وتطوير أنظمة الحماية. لكن عدم تجهيز هذه التقنية بالشكل الصحيح قد يشكل خطرا على شبكة المنظمة!، لأن هذه الخوادم تحاول محاكاة الخدمات المقدمة من الشبكة، وبدلا من أن تكون محاكاة قد تكون تنفيذ فعلي للخدمة[3].

الـمــــلـحـــق

<u>برامج حماية الشبكات</u>

الملحق: برامج حماية الشبكات

أهم برامج حماية الشبكات

إن كنت الشخص المسؤول عن أمن الشبكة في شركتك، فلا بد أنك تشعر بحاجة دائمة وملحة للحصول على عدد كبير من المعاونين، فالوقت لا يتسع إطلاقاً لتهيئة الشبكة للتعامل مع العدد الهائل من المخترقين المحتمل وجودهم على محيطها.

أظهر استطلاع للرأي أجراه "معهد أمن الحواسيب (Computer Security Institute) "بالتعاون مع مكتب التحقيقات الفدرالية (FBI) في الولايات المتحدة، في العام 2003، حول الأمن وجرائم الحواسيب، أن تكاليف الهجمات عبر الإنترنت باهظة جداً، كما هو متوقع. فقد أعلنت 250 مؤسسة شاركت في هذه الدراسة السنوية التي تجرى للعام الثامن على التوالي، عن خسائر بلغت 202 مليون دولار، نتيجة أسباب تراوحت بين المعلومات ذات الملكية الخاصة، وهجمات حجب الخدمة (DoS) ، والفيروسات، وإساءة استخدام الموظفين داخل الشركة لحقوق الوصول إلى الشبكة.

كيف يمكنك أن تحسن من المستوى الأمني لشبكتك؟

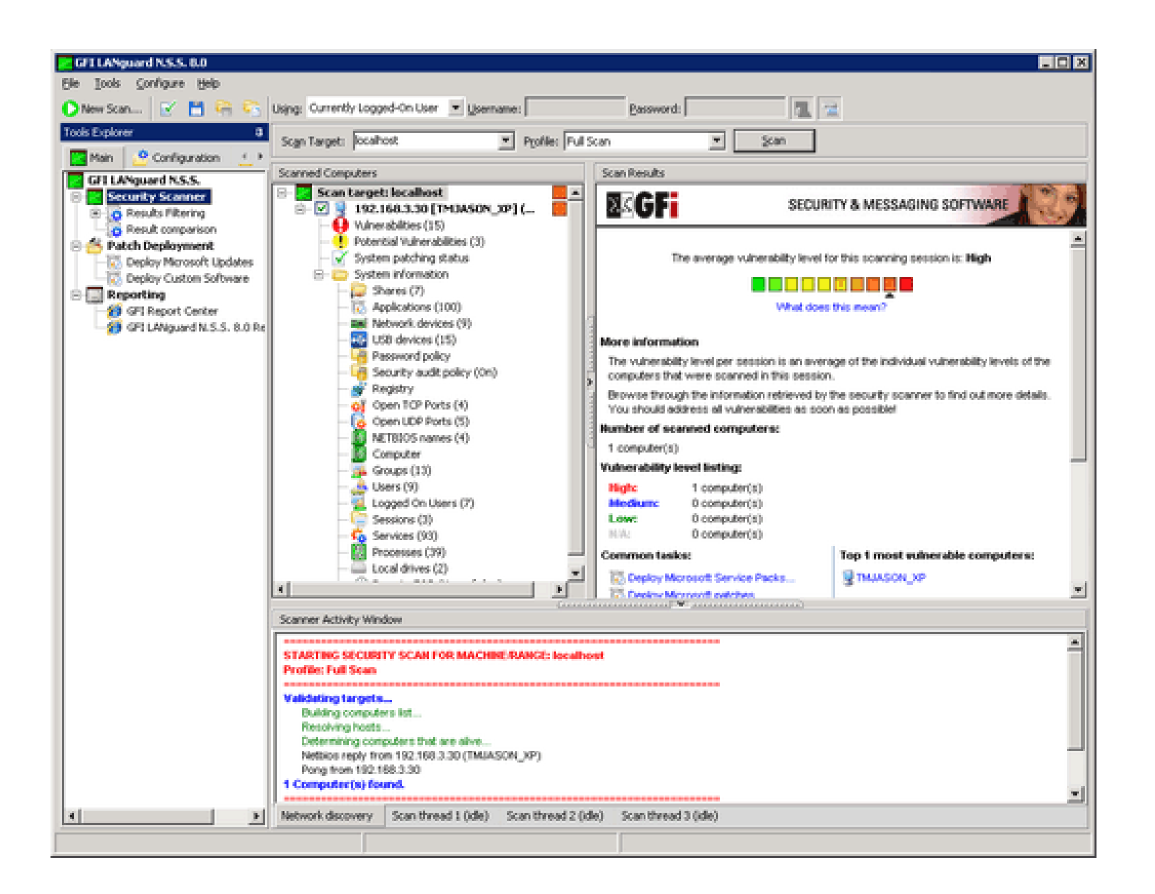
من الواضح أن الخطوة الأولى تكمن في تحديد نقاط الضعف التي يعاني منها نظامك. ولا تكتفي برامج "فحص الشبكات وتقييم نقاط الضعف الأمنية (vulnerability assessment scanners) "بكشف الأخطاء الأمنية الموجودة في الشبكة تلقائياً، بل يمكنها أيضاً أن تصحح تلك الأخطاء أحياناً. وعلى الرغم من توفرها منذ سنوات، لم تنضج هذه الأدوات إلا مؤخراً، فقد تحولت إلى منتجات شاملة وسهلة الاستخدام، على الرغم من كونها معقدة قليلاً، حيث أصبحت توفر مزايا كإنشاء تقارير مفصلة حسب رغبة المستخدم، وتقييم الأخطار عبر أجهزة موزعة، والتصحيح التلقائي للمشاكل المحتملة. ويمكن لبرامج الفحص هذه أن تحدد الاختلالات البرمجية، والفيروسات، ونقاط الضعف في سياسات التحكم بالوصول، وتشمل نقاط الضعف الشائعة في محطات العمل:منافذ NetBIOS المفتوحة، وخيارالمشاركة على الملفات والطباعة(File and Printer Sharing) ، بالإضافة إلى المشاكل الناجمة عن تشغيل مزودات ويب غير مؤمّنة، أو تشغيل زبائن شبكات الند للند (peer to peer). وتستطيع برامج حماية الشبكات كذلك أن تكتشف الإعدادات غير السليمة للتطبيقات، التي يمكنها أن تترك

الشبكة مكشوفة دون حماية. فقد كانت الإعدادات القياسية لمزود البريد الإلكتروني Exchange من مايكروسوفت مثلاً، تجعل المزود يعمل كبدالة لبروتوكول نقل البريد البسيط(SMTP) ، ما يجعله متاحاً للاستغلال من قبل مرسلي البريد الإلكتروني التطفلي (spam) ويؤدي هذا الأمر إلى "اختطاف" المزود واستخدامه لإرسال ملايين رسائل البريد الإلكتروني التي تظهر كبيانات شرعية تنتقل خلال الشبكة الضحية.
وتقدم بعض برامج فحص الشبكات كذلك، إمكانية إدارة عمليات تركيب الرقع الأمنية

(patch management) أو نشر تحديثات للبرمجيات تهدف لتصحيح أي اختلالات برمجية في التطبيقات، علماً أن مزودات ويب ومزودات البريد الإلكتروني وأنظمة التشغيل، تتطلب تركيب الرقع الأمنية بشكل متكرر، وهو أمر يظهر جلياً في منتجات شركة مايكروسوفت ، كونها منتجات يكثر استهدافها .لكن يدور جدل حالياً حول شدة تعقيد برمجيات إدارة تركيب الرقع الأمنية، الأمر الذي لا يسمح بالاعتماد عليها وحدها لإنجاز المهمة، تركز جولتنا على ستة من برامج "حماية الشبكات وتقييم نقاط الضعف الأمنية "التي تستخدم لتحديد نقاط الضعف المحتملة في خدمات الشبكات التي تعتمد على بروتوكول نقل النص المتشعب (HTTP)، وبروتوكول نقل الملفات(FTP) ، وبروتوكول نقل البريد البسيط (SMTP) وتسمح هذه الأدوات لمدراء الشبكات بالتعامل بسرعة مع القضايا الأمنية، وهي تتمتع بسهولة التطبيق كونها لا تتطلب تركيب برنامج زبون على كل جهاز سيخضع للفحص. فبرامج حماية الشبكات وتقييم المخاطر التي تعتمد على برامج زبونة تتطلب تركيب برنامج صغير على كل جهاز، لجمع معلومات أكثر تفصيلاً عن نقاط الضعف الأمنية التي يعاني منها، وتجمع هذه البرامج الزبونة معلومات حول نقاط الضعف على مستوى النظام (عوضاً عن نقاط الضعف على مستوى التطبيقات أو الخدمات)، مثل صلاحيات الملفات، وخصائص حسابات المستخدمين ، وإعدادات سجلّ النظام (Registry) ، وإعدادات التطبيقات، ثم ترسلها إلى قاعدة بيانات مركزية، وهي بذلك تقلل من حجم البيانات التي تنتقل عبر الشبكة مقارنة ببرامج فحص الشبكات التي لا تعتمد على برامج زبونة، ويوفر لهذا السبب، برنامج Security Analyzer 5.0 من شركة NetIQ الخاضع للاختبار في جولتنا إصدارة اختيارية تعتمد على استخدام برامج زبونة، لم نختبر في هذه الجولة أدوات تقييم المخاطر الأمنية التي يمكن استخدامها من خلال الإنترنت، كالأداتين اللتين تقدمهما شركتا Found stoneو Quays تجري هذه الأدوات فحصاً لشبكتك من الخارج، بفحص عناوين IP من الإنترنت لتحديد التهديدات الخارجية، لكن أصبح اليوم بإمكان عدد متزايد من هذه الخدمات أن تقيّم أيضاً

الأنظمة الداخلية في الشبكة ونقاط الضعف الأمنية التي تعاني منها، نختبر في جولتنا هذه، قدرة كل من برامج الفحص التي تعمل عبر الشبكة مباشرة على تقييم الأخطار وإنشاء التقارير، وعلى تصحيح مواضع نقاط الضعف التي قد تؤدي إلى نشوء بيئة حوسبة غير آمنة. وألقينا كذلك، نظرة على أداتين مجانيتين لفحص الشبكات، بالإضافة إلى أداة للتدقيق في شبكة، وجهاز عتادي للأمن.

البرنامج: GFI LAN guard Network Security Scanner 3.3



شكل(1): برنامج GFILANguard Network Security Scanner

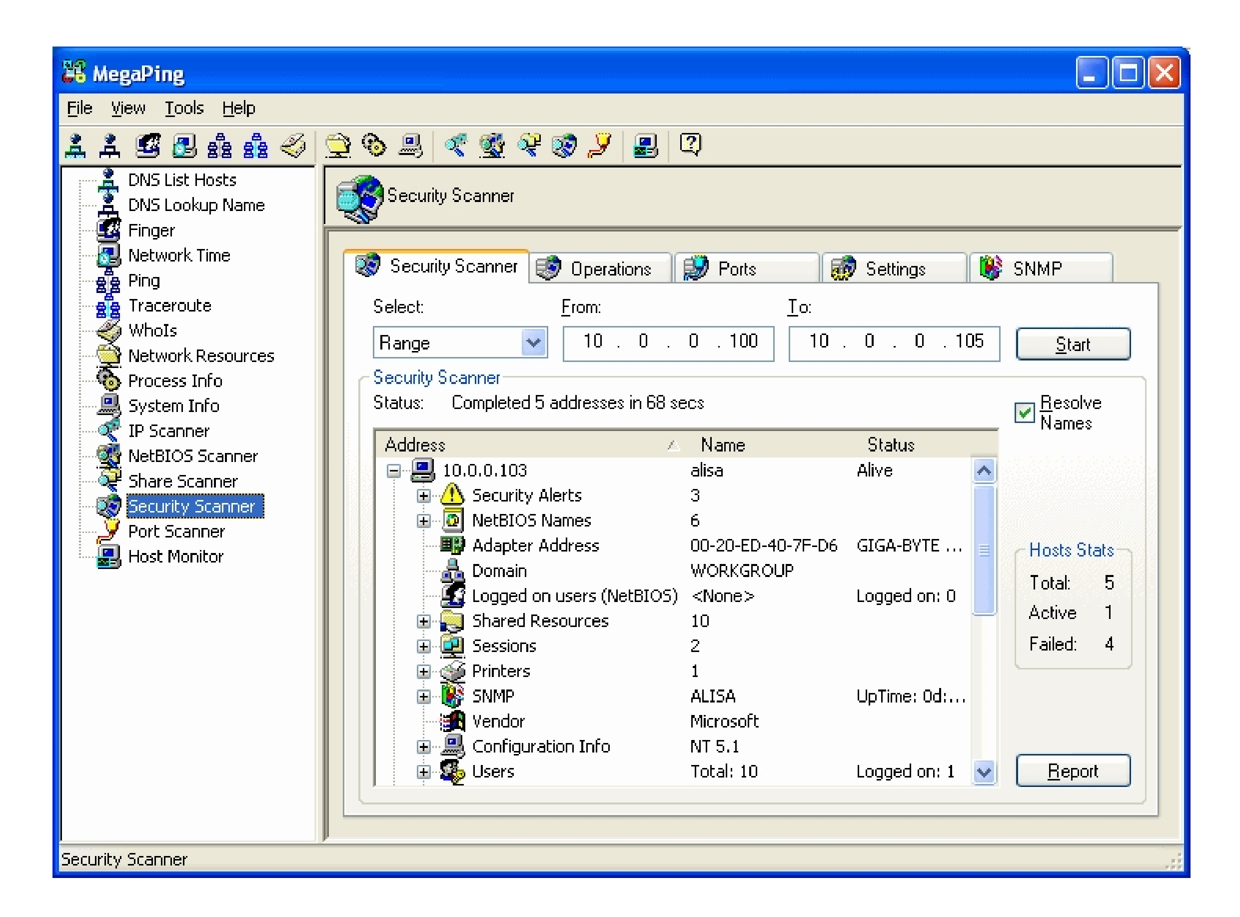
يغطي برنامج GFI LAN guard Network Security Scanner 3.3 مهام فحص الأخطاء الأمنية الأساسية بشكل جيد، إلا إنه يفتقر لبعض القدرات المتطورة المتوفرة في المنتجات الموجهة بشكل أكبر نحو الشركات، مثل برنامج Retina Network Security Scanner من شركة e Eye وبرنامج Security Analyzer 5.0 من شركة.NetIQ فهذا البرنامج لا يستطيع أن يقدم نظرة معمقة حول النصوص البرمجية

لواجهة البوابة العامة (CGI) ، وهي ميزة متوفرة في برنامجRetina ، كما لا يمكنه فحص بعض أنواع عتاد الشبكات، كالروترات (routers) لكن تكاليفه تبقى أقل كثيراً من تكاليف منتجات شركتي eEye و NetIQ، فإذا رغبت في تنفيذ عملية فحص أساسية، يكفي أن تدخل عنوان IP أو مجالاً محدداً والضغط على زر البدء (Start) ويقدم لك البرنامج أنواعاً عديدة من التشكيلات الأمنية مسبقة التعريف، كإمكانية إجراء الفحص باستخدام "بروتوكول التحكم برسائل الإنترنت (ICMP) فقط لكشف الأخطار، أو فحص جميع المنافذ (ports) المتوفرة، أو فحص وجود أي مشاركة مفتوحة للملفات، أو افتقار النظام لأي رقعة أمنية (patch) ويمكنك كذلك، أن تعرّف تشكيلاتك الخاصة لعمليات الفحص الأمنية، كما يمكن للمستخدم، بدون أن يملك الحقوق الخاصة بمدير النظام في نطاق ويندوز، أن يختار أسماء حواسيب معينة أو عناوين بروتوكول MAC أو منافذ مفتوحة، أو إصدارات أنظمة تشغيل معينة، أو معلومات خاصة ببروتوكول إدارة الشبكات البسيطة (SNMP) ، وذلك من خلال بنية شجرية من النتائج المصنفة حسب عناوين IP للأجهزة، أما إذا كنت تملك حقوق إدارة النطاق كاملاً، فيمكنك أن تحصل على معلومات عن كل نظام بدرجة أكبر من التحديد، مثل الموارد المشتركة، وحسابات المستخدمين ، والخدمات المتاحة، وسياسات كلمات المرور، والمعلومات حول سجلّ النظام، والرقع الأمنية المركبة، ويمكن أن تتضمن عملية الفحص أيضاً، البحث عن محاولات إساءة استخدام واجهة البوابة العامة (CGI)بالإضافة إلى الأخطار الأمنية المتعلقة ببروتوكول نقل الملفات (FTP) أو نظام أسماء النطاقات (DNS) أو البريد، أو الخدمات، أو سجلّ النظام. وتصنَّف النتائج ضمن مجموعات حسب فئات محددة، وتتضمن إما توصيات بالخطوات الواجب إتباعها أو العلاج المتاح، أو وصلة مرجعية إلى موقع نظام تتبع الثغرات الأمنية BugTraq أو إلى موقع قاموس "نقاط الضعف والاكتشافات الأمنية الشائعة (CVE) "الذي يعطي لكل ثغرة أو خطر أمني معروف اسماً رسمياً شائعاً، أو إلى إحدى نشرات مايكروسوفت الأمنية (Microsoft Security Bulletin) على الإنترنت. ويمكنك أن تنشئ تقاريرك الخاصة وأن تحفظها باستخدام أداة توليد التقارير، بحيث تلبي احتياجاتك الأمنية بالتحديد، فيمكنك مثلاً توليد تقرير حول جميع الأنظمة التي يكون فيها المنفذ 80 التابع لبروتوكول التحكم بالإرسال (TCP) مفتوحاً عبر الإنترنت، أو التي يكون فيها المنفذ 21 مفتوحاً عبر بروتوكول نقل الملفات (FTP)ويتضمن البرنامج، ومثله برنامجا Retina و SAINT 5، برنامجاً خدمياً يسمح لك بمقارنة تقريرين مع بعضهما، بحثاً عن أي مدخلات جديدة أو محذوفة أو متغيرة، بالإضافة إلى توضيح أي تغيير يطرأ على

التحذيرات أو التحديثات المتاحة، وتسوق الشركة المنتجة برنامج LANguard على أنه حل لنشر وإدارة الرقع الأمنية، ويعمل البرنامج خلال فحص شبكة ويندوز على تحديد الرقع الأمنية التي تم تركيبها على الأنظمة، وبالتالي تحديد الرقع الأمنية الناقصة، وذلك بالاعتماد على معلومات بالتنسيق بين شركة GFI ومايكروسوفت، ويمكن للبرنامج أن ينشر الرقع الأمنية (التي تطلق مايكروسوفت عليها اسم "إصلاحات ساخنة hot fixes "بالإضافة إلى نشر رزم الخدمات(service packs) ومن الجدير ذكره هنا، هو أن عملية إدارة الرقع الأمنية تعتبر عملية معقدة ومتعددة الأوجه، ويحبذ لذلك ألا تعتمد فحسب على برنامج فحص الثغرات الأمنية لتحديد التحديثات الواجب تركيبها بضغطة زر، فالشركات الكبرى مثلاً، تعتمد على برامج النشر التابعة للتطبيقات التي تملكها أصلاً، مثل برنامج Unicenter من شركة Computer Associates، أو برنامج Tivoli من IBM لتحديث الأنظمة المرتبطة بنقطها الشبكية، وذلك من خلال تركيب الرقعات الأمنية، أما بالنسبة للشركات التي لا تملك مثل هذه البرامج، فيعتبر تشغيل برنامج "تحديث ويندوز (Windows Update) "على كل من النقط الشبكية أفضل الحلول المتوفرة من الناحية الأمنية. ونحن ننصح الشركات من مختلف الأحجام، أن تحلل بدقة كل رقعة أمنية قبل نشرها على أجهزتها، لمنع وقوع أي تضارب محتمل مع التطبيقات والخدمات المركبة أصلاً على هذه الأجهزة، يتوفر برنامج LANguard كإصدارة تجريبية لمدة 30 يوماً، بحيث تتوقف بعض المزايا عن العمل بعد انقضاء هذه المدة، مثل علميات الفحص المجدولة للعمل في وقت محدد، وأداة توليد التقارير، وميزة مقارنة النتائج، وتنزيل التحديثات الأمنية عبر الإنترنت، ونشر الرقع الأمنية الخاصة بنظام ويندوز، إلا إذا اشترى المستخدم رخصة لاستخدام البرنامج. ويعتبر المنتج خياراً جيداً بالنسبة لمدراء النظم الذين

يحتاجون لبرنامج فحص أساسي وسريع ومنخفض التكاليف [موقع ويب www.magnetosoft.com]

البرنامج:MegaPing



شكل(2): برنامج MegaPing

يشبه برنامج MegaPing من شركة Magneto Software برنامج LANGuard في كونه أداة جيدة لتنفيذ عمليات فحص الشبكات الأساسية، خاصة إذا نظرنا إلي سعره المنخفض، لكن لا يقدم هذا المنتج عدداً كبيراً من الفحوصات، بالإضافة إلي أن الفحوصات التي يمكنه إجراءها على أنظمة لينكس أو يونيكس لا تتعدى فحص نقاط الضعف المتعلقة بالمنافذ، ويتضمن برنامج Mega Ping أدوات مستقلة تعمل على إجراء الفحوصات بحثاً عن معلومات محددة. وتسمح لك أداة فحص عناوين IP بفحص مجال محدد من العناوين، لتتعرف على العناوين الفعّالة، ثم تعمل على استخلاص أسماء الأجهزة التي تمثلها هذه العناوين،

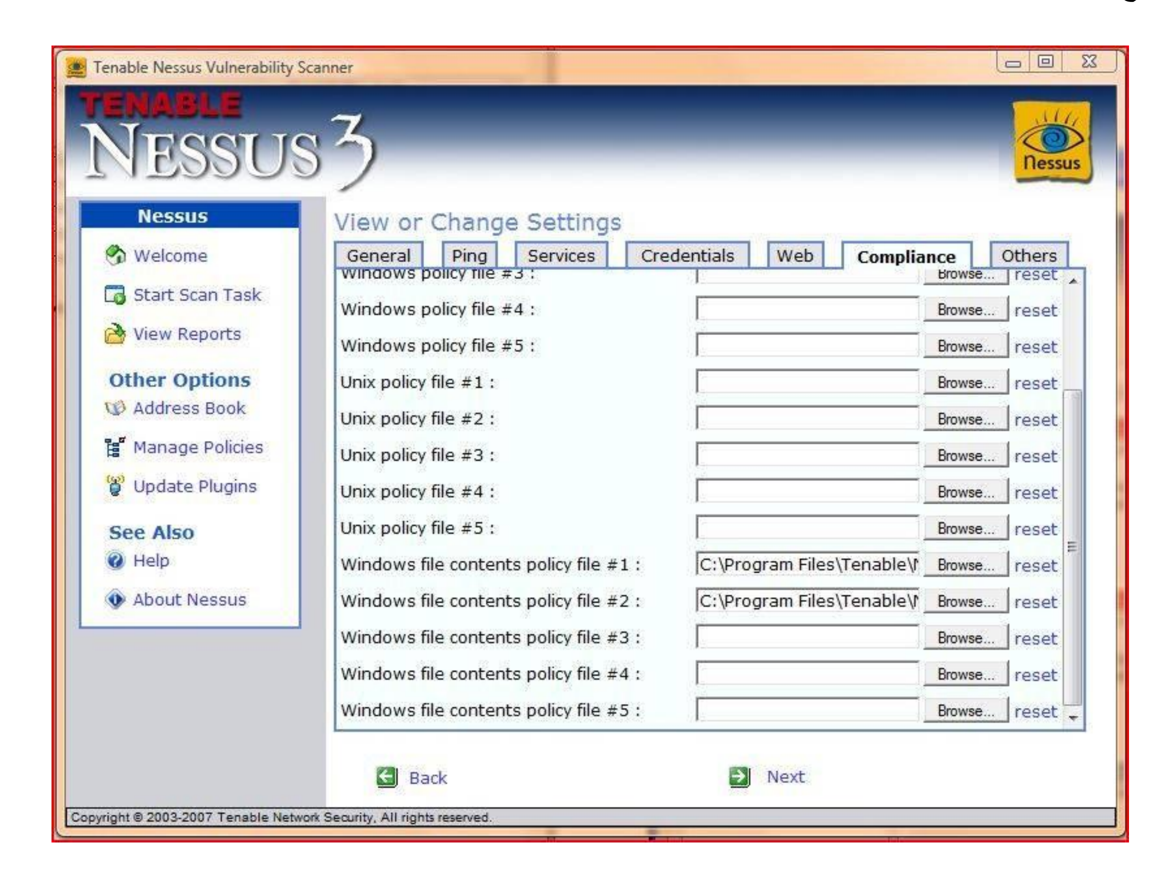
عند تفعيل الخيار الموافق. كما تتيح أداة فحص خدمات بروتوكول NetBIOS أن تفحص مجالات محددة من عناوين IP والأجهزة المستقلة .كما يمكن فحص نطاق (domain) بأكمله، واستخلاص عناوين بروتوكولMAC ، أو أسماء الأجهزة المتصلة بالشبكة حسب بروتوكولNetBIOS ، أو أسماء المستخدمين المتصلين بالشبكة لحظة إجراء الفحص، وتسمح أداة فحص الموارد المشتركة (Shared Scanner) باكتشاف الموارد المشتركة ضمن مجال محدد من عناوين IP أو ضمن نطاق معين، وتتيح أخيراً، أداة فحص المنافذ التي تعتبر آخر أداة مستقلة يتضمنها البرنامج، بفحص مجال من المنافذ، بما في ذلك كل من المنافذ المخوّلة (authorize d ports) التي تتشكل من المنافذ الشهيرة والديناميكية والخاصة المسجلة في النظام، والمنافذ القابلة للاختراق (hostile ports) التي عادة ما يستخدمها المخترقون في محاولات اختراق الأنظمة، وتظهر نتائج الفحص المنافذ المفتوحة التي تمكن البرنامج من التعرّف عليها على جميع الأنظمة التي شملها الفحص، بالإضافة إلى قائمة تظهر الاستخدامات الممكنة لكل منفذ، سواء العادية منها أو القابلة للاختراق، وتستطيع كل وحدة من وحدات الفحص المستقلة أن تنشئ تقارير اختيارية يمكن حفظها إما بهيئة HTMLأو كهيئة نصية (TXT) ولكن خلافاً لبرامج LANguard و Retina و5 SAINT، لا يتضمن برنامج MegaPing أداة خدمية للمقارنة بين عمليات الفحص المتعددة، أو لإعلام جهات أخرى بنتائج الفحص، كإعلام قائمة من المزودات أن المنفذ 25 لبروتوكول نقل البريد البسيط (SMTP) قد وجد فيها مفتوحاً.

كما تستغرق عملية الفحص كاملة كثيراً من الوقت نسبياً، خاصة إذا كنت ترغب بإجراء عملية فحص شاملة لشبكتك، لكن يقدم البرنامج، لحسن الحظ، إمكانية تشغيل كل فحص بشكل مستقل، ثم إنشاء تقرير منفصل عنه، ويستطيع برنامج MegaPing، خلافاً لبعض البرامج الخاضعة للاختبار في جولتنا، أن يبين للمستخدم حالة جميع منافذ بروتوكول "التحكم بالإرسال (TCP) "وبروتوكول "إبراق البيانات للمستخدم (UDP) "في كل من الأنظمة الخاضعة للفحص، وعلى الرغم من أن معظم برامج الفحص تعمل على تحليل الأجهزة عن بعد، إلا أنه من المفيد التعرف على المنافذ المفتوحة في هذه الأجهزة، وعلى المنافذ التي تحاول التنصت على نظامك محلياً، ويمكنك، إذا كنت تملك حقوقاً إدارية مناسبة للنظام، أن تستخدم البرنامج لتجري فحصاً لوجود الرقع الأمنية التي تنتجها مايكروسوفت في الأجهزة التي تتضمن أنظمة ويندوز، وتركيب هذه الرقع عند اللزوم. لكن كما ذكرنا في مراجعة برنامج LANGuard، فإننا لا ننصح أن يعتمد مدير النظام على برنامج

فحص نقاط الضعف الأمنية فقط، للقيام بمهمات إدارة تركيب الرقع الأمنية، يتضمن برنامج MegaPing أيضاً، عدداً من البرامج الخدمية الإضافية التي لا تتعلق بفحص الجانب الأمني للشبكة، مثل: أدوات البحث عن اسم محدد في نظام أسماء النطاقات (DNS) ، وأمر تتبع الطريق (trace route) وأمر finger و pingوأمر التعرف على اسم مالك عنوان IP محدد(Whois) ، والتعرف على زمن الشبكة (network time)، بالإضافة إلى مجموعة من أدوات إنشاء التقارير حول العمليات الفعالة في النظام، التي تشبه بعملها عمل برنامج Windows Task Manager الموجود في نظام ويندوز، لكنها تمتاز بتطور أكبر، وتعتبر هذه جميعاً من الأدوات التي لا يمكن لمدير النظام أن يستغني عنها. ويمكنك تنزيل إصدارة تجريبية من البرنامج لمدة 30 يوماً من موقع الشركة المنتجة، يقتصر عملها في مراقبة وفحص الجانب الأمني لخمسة أجهزة.

يعتبر برنامج MegaPing، مثله مثل برنامج LANGuard ملائماً للاحتياجات الأساسية لمدراء النظم في مجال فحص الشبكات، لكن بتكلفة قليلة. وسيعجب البرنامج مدراء النظم الذين يفضلون امتلاك برامج خدمية منفصلة لتلبية احتياجاتهم ، عوضاً عن مجموعة الفحوصات الأكثر اتساعاً التي يقدمها برنامج LANGuard. [موقع ويب www.magnetosoft.com]

البرنامج: **Nessus**



شكل(3): برنامج Nessus

لا تضاهي أي من المنتجات الأخرى هذا البرنامج للفحص الأمني عن بعد، من ناحية القيمة التي يقدمها، فهو مجاني يهدف مشروع Nessus الذي يتبع مبدأ المصادر المفتوحة، حسب تصريح ريناود ديرايسون الذي يرجع فضل إنشائه إليه، إلى "توفير برنامج فحص أمني عن بعد لمجتمع الإنترنت، يتمتع بالقوة وسهولة الاستخدام، وسرعة التحديث والمجانية"ويقدم البرنامج فعلاً، مجموعة قيّمة من إعدادات وخيارات الفحص، على الرغم من أنها قد تبدو أكثر من المطلوب بالنسبة لبعض المستخدمين، وقد يحتاج مدير النظام إلى تكريس كمٍ كبير من الوقت لتعلم النواحي المعقدة من البرنامج ليتمكن من استخدامه بفعالية أكبر، بني برنامج Nessusاعتماداً على معمارية الزبون/ المزود، وهو يتيح للمستخدم تشغيل برنامج إدارة النظام، الذي يعمل على إجراء فحوصات لنقاط الضعف الأمنية، وإنشاء وتخزين قواعد بيانات بتلك الفحوصات على جهاز آخر غير المزود، وتتوفر إصدارات زبونة من البرنامج لواجهة جافا وواجهة ويندوز (Win32)، وواجهةX11 ، ما

يجعل البرنامج فعلاً، أداة متعددة المنصات، يمكنها فحص أنظمة لينكس، وويندوز، ويونيكس، ويقدم البرنامج كماً مذهلاً من الفحوصات المخصصة، على شكل برامج مضافة (plug–ins) وتقدم هذه البرامج المضافة فحوصات مثيرة للاهتمام يمكنها البحث عن نقاط الضعف في أجهزة الروترات التي تنتجها شركة Cisco وغيرها من الشركات، بالإضافة إلى فحص نصوص CGI البرمجية، وأخطاء طوفان الذاكرة الوسيطة للشيفرة البرمجية(buffer overruns) ، ووصلات الوصول عن بعد، والأبواب الخلفية (backdoors) التي قد تتركها البرامج، وبروتوكول "استدعاء الإجراءات عن بعد(RPC) "، وبروتوكول إدارة الشبكات البسيطة(SNMP).

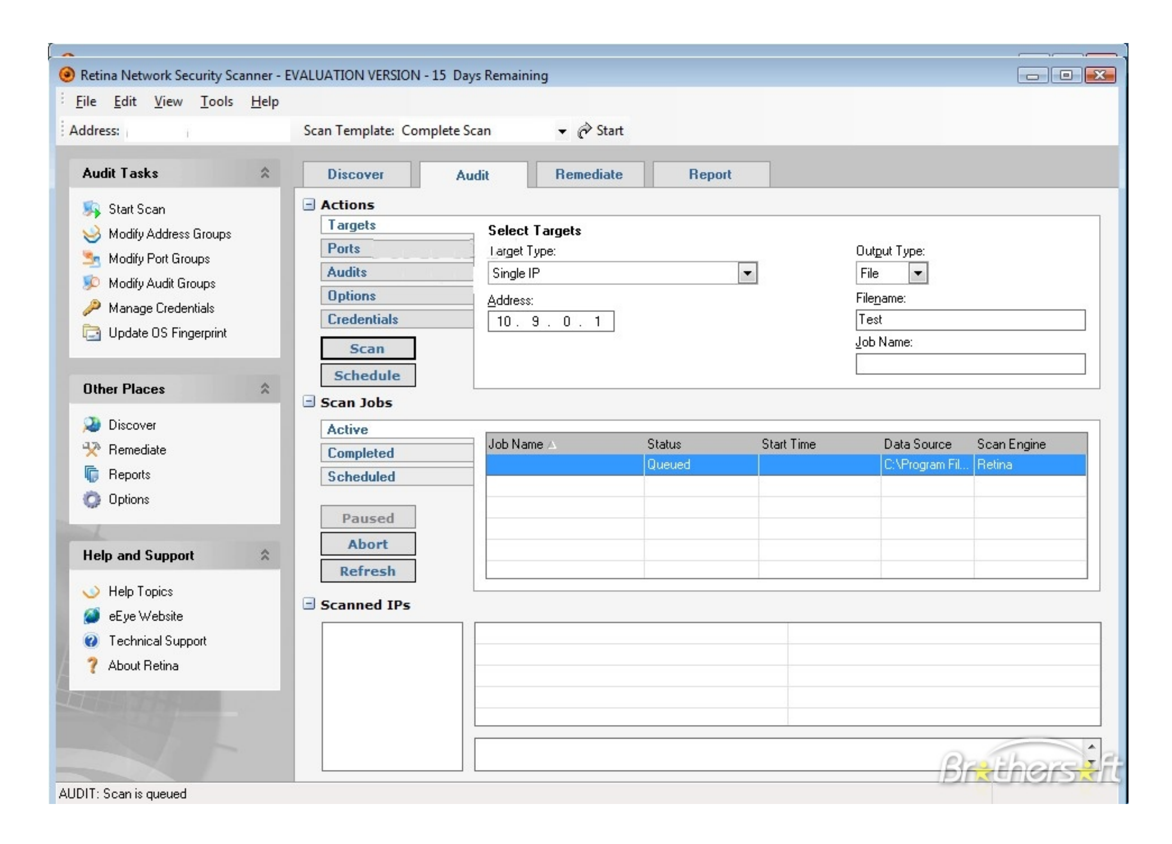
ركّب البرنامج على محطة عمل تعتمد على نظام التشغيل Red Hat Linux 9 وكانت المفاجأة السارة هي سهولة إتمام مهمة التركيب من خلال النصوص البرمجية الخاصة بالعملية، وهو أمر غير معتاد في عالم برمجيات المصادر المفتوحة، استخدم بعد إنهاء عملية التركيب، الأدوات التي تعتمد على الأوامر السطرية (command line)لإضافة مستخدم أوليّ للنظام، ولتوليد مصدّقة خاصة بكل جهاز زبون. واستطعنا بعد ذلك أن نشغّل برنامج Nessus وأن ندخل إلى واجهة استخدام نظام X11 بدون حدوث أية مشاكل، ويمكنك إما تعديل إعدادات عملية الفحص حسب رغبتك، أو أن تستخدم إعداداته القياسية، غير أن تعديل الإعدادات يستغرق وقتاً كبيراً نسبياً من مدير النظام، وذلك بناء على مدى تنوع الشبكة والأجهزة المرتبطة بها، ويمكنك أيضاً، أن تصنف إعدادات فحص منافذ النظام ضمن مستويات متعددة، لتتيح للبرنامج أن يأخذ في حسبانه عند إجراء الفحص وجود الجدران النارية وأنظمة تحرّي وجود محاولات الاختراق(intrusion detection) ، ونقترح عليك، لتحصل على معلومات أكثر دقة وتفصيلاً حول الأجهزة التي تتضمن أنظمة ويندوز ضمن نطاق شبكة ويندوز، أن تنشئ حساباً جديداً ومجموعة مستخدمين جديدة للنطاق، ومنحهما صلاحية الوصول إلى سجلّ النظام عن بعد، ولا يتيح لك هذا الأمر أن تصل إلى إعدادات سجلّ النظام فحسب، بل أن تصل كذلك إلى مستويات الرقع الأمنية ورزم الخدمات (service packs) المركبة، وإلى نقاط الضعف الأمنية في المتصفح إنترنت إكسبلورر، وإلى الخدمات الفعّالة في النظام الخاضع للفحص، ويتم عرض نتائج الفحص مصنفة حسب النطاقات والأجهزة ونقاط الضعف الأمنية في كل منها، وتظهر التقارير إلى جانب نقاط الضعف التي وُجِدت، عدداً كبيراً من الاقتراحات التي تشرح طبيعة المشكلة بالإضافة إلى سرد الحلول الممكنة .وتظهر النتائج أيضاً، وصلات إلى قاموس "نقاط الضعف والاكتشافات الأمنية الشائعة "

(Common Vulnerabilities and Exposures, CVE)في الموقع www.cve.mi tre.org الذي يسرد قوائم بنقاط الضعف الأمنية المعروفة، وإلى موقع شبكة TechNet من مايكروسوفت في الموقع www.microsoft.com/technet الذي يعتبر مورداً مهماً عبر الإنترنت لمدراء تقنية المعلومات، وتوفر هذه الميزة لمدراء النظم إمكانية الحصول على معلومات من موارد مهمة وإمكانية تنزيل الرقع الأمنية اللازمة، لكننا لاحظنا أن الخلاصات التي يقدمها البرنامج ضمن التقارير، تفتقر قليلاً إلى المرونة في التعامل، كما لا يقدم البرنامج النتائج مصنفة ضمن مجموعات حسب منهجيات تصنيف مختلفة، كتصنيفها حسب نقاط ضعف أمنية محددة، أو نوع أنظمة التشغيل في الأجهزة، أو شدة الخطورة، مثلما هو متوفر في برنامج Security Analyzer 5.0 من NetIQ وفي برنامج5 SAINT، لكن يمكنك إنشاء التقارير بواحد من 6 هيئات مختلفة، بما في ذلك المخططات الدائرية (pie chart) والجداول، ما يتيح لك الإطلاع على النتائج من منظور ذي مستوى أعلى، وهو أمر ضروري أحياناً. لكن على الرغم من ذلك، تؤدي حقيقة افتقار البرنامج لإمكانية عرض النتائج مصنفة حسب نوعها، إلى التقليل من تنوع الهيئات المتاحة لعرض التقارير.

سيعجب برنامج Nessus معظم مدراء النظم الذين يرغبون بالحصول على أداة فحص شاملة بالإضافة إلى الحصول على معرفة معمقة وطويلة الأمد في مجال الأخطار الأمنية التي تتعرض لها الشبكات.

[موقع ويبwww.nessus .com]

البرنامج: **Retina Network Security Scanner**



شكل(4): برنامجRetina Network Security Scanner

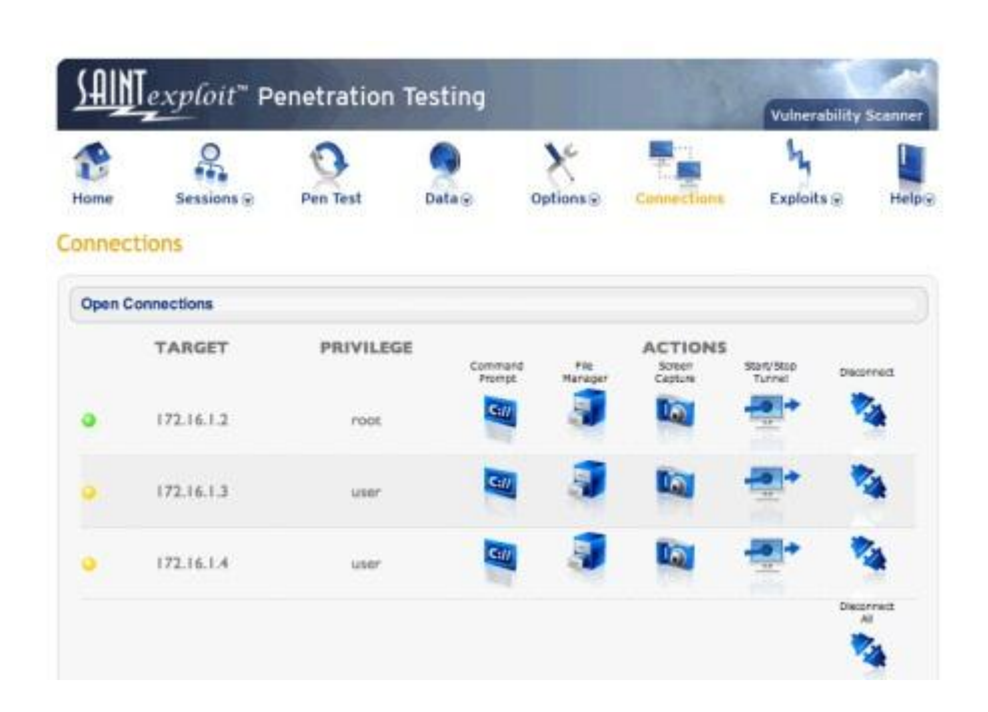
يعتبر برنامج Retina Network Security Scanner من شركة eEye Digital Security أداة مكتملة الميزات وجيدة التنظيم ومتعددة الأوجه لفحص وجود نقاط الضعف الأمنية في الشبكات، وهو يقدم فحوصات لنقاط الضعف الأمنية التي تعاني منها أنظمة لينكس ويونيكس وويندوز، بالإضافة إلى قدرته على إصلاح الكثير من المشاكل التي يكتشفها تلقائياً، كما يتيح للمستخدم إنشاء فحوصات مخصصة حسب رغبته، وقد مكنت هذه المزايا برنامج Retina من نيل قصب السبق، وانتزاعه لقب خيار المحررين في هذه الجولة، وتعتبر ميزة "الإصلاح التلقائي" واحدة من أكثر أدوات برنامج Retina إثارة للإعجاب، وهي ميزة فريدة بين المنتجات المختبرة الأخرى، فهي تتيح لمدراء النظم الذين يملكون صلاحيات مناسبة أن يصلحوا، بنقرة واحدة، أعطال سجلّ النظام (registry) ومشاكل صلاحيات المستخدمين المتصلين بالشبكة عبر العقد

الشبكية عن بعد، وتكمن الميزة المثيرة الأخرى التي يقدمها البرنامج في أداة التدقيق الفريدة التي يتضمنها، والتي تسمح للمستخدم أن يطور استعلامات مخصصة حول نقاط الضعف الأمنية التي يعلم بوجودها في شبكته ، لكن يعتبر Retina برنامج فحص الشبكات الوحيد في جولتنا الذي يتضمن هذه الوظيفة التي تتيح كشف نقاط الضعف المعروفة، حيث يمكنك إنشاء فحص تدقيقي مخصص باختيار منهجية معينة من بين تشكيلة من الفئات، تتضمن عدداً من الخدمات الشائعة والمزودات وحتى نقاط الضعف الأمنية المتعلقة بالتجارة الإلكترونية، أو يمكنك إنشاء فحوص تدقيقية خاصة بك بالكامل، وتضمينها لاحقاً كجزء من عملية الفحص الشاملة، ثم أن توجه هذه الفحوص بحيث يتم تطبيقها على أهداف مختارة .ويمكنك تحديد خيارات معينة للفحوصات، كفحص إصدارات محددة من البرمجيات، أو فحص نصوص برمجية لواجهة البوابة العامة (CGI) ، أو الرقع الأمنية، أو مدخلات سجلّ النظام، كانت عملية تركيب البرنامج مباشرة، وأجرى خلالها برنامج Retina عملية مزامنة لقواعد بيانات تعريف نقاط الضعف الأمنية مع مزود شركة eEye وفور تشغيل البرنامج ستلحظ أن واجهة الاستخدام تتيح الوصول إلى 4 وحدات، هي :المتصفح (browser)، والمتتبع(tracer) ، والمنقِّب(miner) ، والفاحص (scanner) يسرد متصفح ويب المدمج في البرنامج جميع عناصر الصفحات على شكل بنية شجرية، ثم يجري المتتبع عملية "تتبع الطريق trace " (routeلكل منها، ثم يظهر نتائج أزمنة الاستجابة. أما وحدتا المنقِّب والفاحص، فيشكلان الدماغ المفكر في عمل البرنامج، حيث يحاول محرك الذكاء الصناعي الذي أنتجته الشركة، والذي تعتمد عليه وحدة المنقِّب أن يحاكي سلوك المخترق من خلال مهاجمة نقاط الضعف الأمنية، وقد كانت وحدة الفاحص إحدى أفضل الوحدات المماثلة بين البرامج المختبرة، من حيث السرعة والدقة، وبعد أن تعرّف الجهاز المراد فحصه أو المجال المحدد من عناوينIP ، تعمل وحدة الفاحص على كشف جميع العقد الشبكية التي تعطي رد فعل يدل على وجودها، ثم إجراء مجموعة من الفحوصات مسبقة التعريف على هذه الأهداف، وتظهر النتائج بهيئة يمكن تصفحها بسهولة بالغة، بحيث يتم سرد الأجهزة التي خضعت للفحص ضمن إطار واحد، ونقاط الضعف الأمنية المحتملة في إطار آخر لكن لا يسمح البرنامج للأسف بتصنيف النتائج حسب نوع هذه الأخطار.

ويتم تصنيف نتائج الفحص ضمن مجموعات حسب مستوى الخطورة المعرض له كل من الأجهزة الخاضعة للفحص، وتتضمن النتائج، بشكل شبيه ببرنامجي Security Analyzer 5.0 من NetIQ و SAINT 5،

معلومات شديدة التفصيل حول المشكلات التي تم العثور عليها، والحلول الممكنة. ويظهر برنامج Retina وصلات وأرقاماً لتعريف كل من نقاط الضعف الأمنية المكتشفة حسب نظام تتبع الثغرات الأمنية BugTraq وحسب قاموس "نقاط الضعف والاكتشافات الأمنية الشائعة(CVE) "، وحسب نشرات مايكروسوفت الأمنية (Microsoft Security Bulletin)، التي تعتبر جميعاً قوائم مرجعية لنقاط الضعف الأمنية المعروفة، ويبني محرك إنشاء التقارير 3 أنواع من المخططات مسبقة التعريف، هي :التقارير الكاملة، والتقارير التنفيذية المختصرة، والتقارير التقنية، ويمكنك أيضاً، أن تخصص تقريراً بما يلائم متطلباتك الخاصة، وهي ميزة تغيب عن جميع المنتجات الأخرى في هذه الجولة، باستثناء برنامج SAINT 5 ويقدم برنامج Retina عموماً، أفضل توازن بين المزايا والقوة وقابلية الاستخدام والسرعة بين جميع المنتجات في هذه الجولة [موقع ويب www.eeye.com]

البرنامج: SAINT 5



شكل(5): برنامج SAINT 5

يتوفر برنامج SAINT 5 لمنصات نظامي يونيكس ولينكس فقط، ويعتبر أحد أكثر برامج فحص وجود نقاط الضعف الأمنية تعقيداً في هذه الجولة، ويمكنك تعديل إعدادات هذه الأداة بشكل بالغ الكثافة، حيث يمكنك أن تشكّل بتفصيل شديد الفحص الأكثر ملائمة لطبيعة شبكتك، وأن تحدد عمق عمليات الفحص التي ترغب بإجرائها، بل ويمكنك كذلك، إنشاء فحوصات محددة لإجرائها على قواعد البيانات والخدمات والتطبيقات ، لكن أكثر ما أثار إعجابنا في البرنامج هو الشمولية التي يتمتع بها في أسلوب عرضه لنتائج الفحوصات التي يجريها، فقد تضمنت النتائج مثلاً، معلومات تفصيلية ووصلات إلى جميع المصادر الأمنية المتعلقة التي يمكن أن تسلط مزيداً من الضوء على النتائج، كما يتيح البرنامج تعديل النتائج، بحيث يمكن ترتيبها حسب مواصفات محددة، مثل الاسم ونقاط الضعف الأمنية وشدة الخطر الذي تشكله، وعلى الرغم من السمعة السيئة حول صعوبة تركيب تطبيقات نظامي لينكس ويونيكس عامة، إلا أننا وجدنا عملية تركيب البرنامج بالغة السهولة، وفور إتمام عملية التركيب يتم تشغيل البرنامج ضمن نافذة متصفح قياسية، تمتاز بواجهة كثيفة وجيدة البنية. ويتم إلحاق محتوى إعدادات عمليات الفحص بقواعد بيانات يتم إنشاؤها ضمن نظام الملفات التابع لبرنامج الإدارة، بحيث تحتوي كل قاعدة بيانات على بيانات خاصة بعملية الإعداد والنتائج والتقرير المرافق، ما يسهل من ربط ودمج مختلف البيانات التي ينشئها البرنامج، يتمتع البرنامج بميزة مفيدة، تكمن في إمكانية إعداده للدخول إلى نطاقات ويندوز ببساطة، من خلال استخدام اسم المستخدم وكلمة المرور الخاصة بمدير النظام، وذلك لإجراء الاختبارات التي تتطلب التحقق من الهوية قبل الدخول إلى النظام، ويقدم البرنامج، مثله في ذلك مثل Security Analyzer من شركة NetIQ ، عدداً محدداً من الفحوصات مسبقة الإعداد والموجهة، وهي ميزة مفيدة تؤدي إلى توفير الوقت على المستخدم. ومن الأمثلة الجيدة على هذه الفحوصات، فحص "أخطر 20 نقطة ضعف أمنية للإنترنت حسب معهد"SANS "، (SANS Top 20 Most Critical Internet Security Vulnerabilities)، وهو اختبار يفحص جميع العقد الشبكية المستهدفة باحثاً عن أي من الأخطار الأمنية العشرين الأكثر شيوعاً والأكثر خطراً على شبكات الإنترنت حسب معهد "مدراء الأنظمة والشبكات والأمنSANS، ويتم إنشاء تقارير البرنامج، التي تعتبر خارجة عن المعتاد، ضمن برنامج مرفق يسمىSAINT writer ، وهو برنامج فريد ينشئ تقارير مسبقة الإعداد مفصلة بطريقة تلبي احتياجات الموظفين الإداريين والتقنيين، ويتيح لك هذا البرنامج المرفق، بفضل الميزة التي يقدمها لاكتشاف الأنماط المتشابهة، أن تقارن بين نتائج الفحوصات الواردة في تقريرين أو

أكثر، لكن للأسف لا تتوفر ميزة الاستعلام ضمن التقرير، أو إمكانية تصنيف النتائج في مجموعات، وهما ميزتان تسمحان للمستخدم أن يتعرف بدقة على وجود مشاكل محددة، وعلى الرغم من أن ميزة إنشاء التقارير المتوفرة في البرنامج أعمق من مثيلاتها المتوفرة في المنتجات الأخرى في هذه الجولة، إلا أنها قد تؤدي إلى إظهار نتائج كثيفة أكثر من المطلوب، خاصة عند إجراء فحوصات على شبكات كبيرة الحجم. لكن يبقى SAINT 5 عموماً، برنامجاً غنياً بالمزايا، يقدم قدرات تحليلية مكثفة، ونحن ننصح بكل تأكيد أن تأخذ البرنامج في اعتبارك إذا كانت شبكتك تتضمن عدداً كبيراً نسبياً من أنظمة لينكس ويونيكس.

المراجع والمصادر

أولا:الكتب

[1] تركيب وصيانة الشبكات، م.احمد خميس،رقم الإيداع 2009/19610، ISBN:977-17-7580-40

[2] كتاب الشبكات

تأليف: اد تيلور، إعداد: خالد العامري ،رقم الإيداع 2007/16887، ISBN 977-419-816-6

[3] كتاب الخطوة الأولى نحو أمان الشبكات (first-step Network Security)

تأليف: توم توماس ،الطبعة الأولى 2004 ، ISBN 9953-29-065-2

ثانيا:الكتب الالكترونية

[4] الحاسبات و تطبيقاتها في التعليم (COMP 2052)، إعداد: د.يوسف بغدادي ،2009

[5] الموسوعة الحاسوبية، إعداد: د.وليد عودة ، 2009

[6] جزء من كتاب ستولونج في أمنية البيانات، ترجمة فهد آل قاسم ،2010

ثالثا:بحوث التخرج

[7] بحث لنيل الماجستير، بعنوان "دور المواقع الديناميكية في العملية التعليمية" إعداد: م.حسن عبد الله أبكر، 2009-2010

[8] تطبيقات الانترنت، بحث لنيل درجة البكالوريوس في كلية هندسة الحاسوب جامعة أفريقيا. السودان

إعداد: حسن عبد الله أبكر 2000 -2001

[9] بناء نظام تراسل آمن، بحث لنيل درجة البكالوريوس في كلية هندسة الحاسوب .**سوريا**، إعداد: محمود محفوض وآخرون

رابعا:الورقات العلمية

[10] أمن شبكات الحاسب والانترنت،إعداد: حمدان لافي حمدان

[11] أمن الشبكات اللاسلكية،إعداد: ألبرتو اسكادرو باسكال

خامسا: مواقع الانترنت

[12] Ar.wikipedia.org آخر زيارة 14-1-2012.

[13] http://www.elshami.com آخر زيارة 28-1- 2012

[14] http://www.coeia.edu.sa آخر زيارة 05-03-2012

[15] http://labmice.techtarget.com/antivirus/articles آخر زيارة 05-03-2012

[16] http://ar.wikipedia.org/wiki/FTP آخر زيارة 18-03-2012.

[17] http://forums.iraqcst.com/showthread.php آخر زيارة 14-03-2012.

[18] http://www.javvin.com/networksecurity/CommunicationSecurity.html

آخر زيارة 5-03-2012

[19] http://coeia.edu.sa/index.php/ar/tags/network-security.html آخر زيارة 29-01-2012

[20] www.microsoft.com/technet/itsolutions/network/ipsec/default.mspx آخر زيارة 24-3-2012

[21] http://www.all-patch.net/vb/threads آخر زيارة 29-1-2012

[22] http://www.dev-point.com/vb/t90903-2.html آخر زيارة 5-3-2012

[23] www.king-sabri.net آخر زيارة 14-3-2012

[24] http://en.wikipedia.org/wiki/ Transport_Layer_Security.htm آخر زيارة 18-03-2012

[25] http://www.computer.howstuffworks.com/firewall1.htm آخر زيارة 15-3-2012

[26] http://www.boosla.com/showArticle.php?Sec=Security&id=28 آخر زيارة24-03-2012

[27] Microsoft Windows Help and Support آخر زيارة 14-3-2012

[28] http://www.haladeeb.name/category/cryptography/ آخر زيارة14-3-2012

[29] http://coeia.edu.sa/index.php/ar/tags/information آخر زيارة 15-3-2012

[30] http://coeia.edu.sa demilitrized-zone-dmz.html آخر زيارة 2-1-2012

